Vol. 20, n.° 3, pp. 19-46, 2021

Revista UIS Ingenierías

Página de la revista: https://revistas.uis.edu.co/index.php/revistauisingenierias

Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano

Cybersecurity in digital justice: recommendations for Colombian case

Maribel Patricia Rodríguez-Márquez [1]

[1] Escuela Superior de Guerra, Colombia. Correo electrónico: [a] maribelp.rodriguez@esdegue.edu.co
Orcid: 0000-0002-0591-6400

Recibido: 10 octubre, 2020. Aceptado: 24 noviembre, 2020. Versión final: 3 mayo, 2021.

Resumen

La adopción de las tecnologías de la información y las comunicaciones (TIC) ha causado múltiples transformaciones tanto al sector público como al privado. El uso de las TIC en el sector justicia agiliza los procesos judiciales; sin embargo, este uso también constituye un riesgo, por cuanto la justicia es parte de la infraestructura crítica de las naciones; aunado a las características de la información que atañe a los procesos, una interrupción de la prestación de esos servicios sería catastrófica. Por tal razón, la ciberseguridad juega un papel en cada etapa de los procesos judiciales digitales. Así, el objetivo de este artículo es proponer recomendaciones en ciberseguridad aplicables a los procesos judiciales digitales en el caso colombiano a partir del análisis de literatura, que permitió establecer el panorama de la justicia digital con énfasis en Latinoamérica, las TIC que suelen usarse en cada etapa del proceso judicial digital, los riesgos cibernéticos, las recomendaciones para enfrentarlos y cómo las funciones del marco de ciberseguridad de la National Institute of Standards and Technology (NIST) son consideradas.

Palabras clave: justicia digital; ciberseguridad; proceso judicial digital; riesgo cibernético; marco de ciberseguridad; TIC; ciberjusticia; e-justicia; NIST; administración de justicia; justicia colombiana; recomendaciones.

Abstract

The adoption of Information and Communication Technologies -ICT- has caused multiple transformations in both the public and private sectors. The use of ICT in the justice sector speeds up judicial processes. However, this use raises risks since justice is part of the critical infrastructure of nations. In addition to the judicial information' characteristics, an interruption in the provision of these services would be catastrophic. For this reason, cybersecurity plays a role in each stage of digital judicial processes. This paper aims to propose cybersecurity recommendations to digital judicial processes in the Colombian case based on a literature analysis, which described the digital justice landscape with an emphasis on Latin America. It also analyzes which ICT is used in each stage of the digital judicial process, their cyber risks, and the recommendations to face them. Also, how the functions of the National Institute of Standards and Technology –NIST- cybersecurity framework are considered.

Keywords: digital justice; cybersecurity; digital judicial processes; cyber risks; cybersecurity framework; recommendations; ICT; cyberjustice; e-justice; NIST; justice administration; Colombian justice.

ISSN impreso: 1657 - 4583. ISSN en línea: 2145 - 8456, **CC BY-ND 4.0**
Como citar: M. P. Rodríguez-Márquez, "Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano," *Rev. UIS Ing.*, vol. 20, no. 3, pp. 19-46, 2021, doi: 10.18273/revuin.v20n3-2021002

1. Introducción

Desde finales del siglo pasado, el uso de las tecnologías de la información y las comunicaciones (TIC) en diferentes ámbitos ha causado una transformación en las formas de desarrollo de cada uno de tales ámbitos [1], [2]. El sector justicia no es la excepción. El uso de las TIC en el sector justicia, o justicia digital, va desde el uso de archivos electrónicos hasta las videoconferencias para las audiencias en los juicios, entre otros.

La justicia es un servicio público básico e imprescindible, es esencial y hace parte del Estado de derecho. Si se interrumpiera la prestación de justicia, se causaría a la población un altísimo perjuicio, por ello, hace parte de la infraestructura crítica [3]. Si bien, la justicia digital implica beneficios, también hay algunos riesgos. Entre los beneficios están la eficiencia, la transparencia, la reducción de costos y de tiempos [4], [5].

Sin embargo, la información sensible que el sistema judicial maneja constituye un atractivo para los cibercriminales, hackctivistas, entre otros; si la información judicial cae en esas manos criminales, puede llegar a ser muy lesivo para los diferentes usuarios de la administración de justicia [6]. Pese a ello, es poca la literatura que examina las consecuencias de la incorporación de las TIC en los procedimientos de la administración de justicia [7], y más escasa la literatura relacionada con la ciberseguridad en la justicia digital.

Ahora bien, Colombia, desde hace varias décadas, tiene una crisis judicial profunda que no permite que el sistema judicial satisfaga las demandas de la población, por ello, se han implementado varios planes de descongestión y esfuerzos de modernización tecnológica y transformación digital para fortalecer y mejorar el servicio de justicia en el país, a través del impulso del uso de las TIC y de herramientas disruptivas como la analítica de datos y la inteligencia artificial, apoyada en una política de seguridad de la información y protección de datos [8]-[10].

La incursión de estas tecnologías y el atractivo de la información judicial para los cibercriminales propician el objetivo de este artículo, que es proponer recomendaciones en ciberseguridad, aplicables a los procesos judiciales digitales en el caso colombiano, a partir de una revisión de la literatura y de un análisis documental que examinó cuál es el panorama de la justicia digital, cuáles son las TIC que suelen usarse en cada una de las etapas del proceso judicial digital, cuáles son los riesgos cibernéticos y recomendaciones para enfrentarlos, cómo las funciones del marco de ciberseguridad de la NIST son consideradas en las etapas de los procesos judiciales digitales.

Este artículo está estructurado en siete secciones. La segunda y tercera describen los elementos conceptuales sobre justicia digital, ciberseguridad y sobre el marco de ciberseguridad NIST; la cuarta sección describe el método empleado; la quinta presenta y discute los hallazgos; la sexta presenta las recomendaciones que podrían aplicarse al caso colombiano; y la séptima presenta las conclusiones y sugerencias para futuros estudios.

2. Justicia digital

Desde los años 90, son varias las iniciativas de la incorporación de las TIC en la administración de justicia [11], [12]. La justicia digital hace parte del gobierno electrónico, entendido como el uso de las TIC para el desarrollo de una administración pública eficiente, en la prestación de servicios e información a los ciudadanos y empresas [13]-[15].

La justicia digital constituye un sector de la sociedad de la información. Una definición amplia de la justicia digital contempla el uso de las TIC para prevenir el crimen, mejorar la administración de justicia y el sistema legislativo [16], [17]. La justicia digital busca mejorar el acceso de los ciudadanos a la justicia y a la acción judicial efectiva, que consiste en la solución de controversias o la imposición de sanciones penales. La justicia digital también es conocida como justicia electrónica, e-justicia, justicia *on-line* o ciberjusticia.

Los objetivos específicos de la justicia electrónica son: economía y concentración procesal; evitar el rezago de expedientes para hacer más eficiente la impartición de la justicia; incrementar la transparencia; incrementar el acceso a los servicios de justicia; acercar a los ciudadanos y propender por su participación; y reducir los costos de los procesos judiciales [4], [18]-[20].

La justicia digital involucra, desde los métodos de comunicación como el correo electrónico, las videoconferencias, los sistemas de resolución de conflictos en línea, hasta los sistemas de información para la gestión de los procesos, pasando por las tecnologías para los tribunales (salas de audiencia), los servicios en línea para consulta de los ciudadanos, entre otros [16], [21], [22].

La justicia digital, además, implica el desarrollo del marco regulatorio necesario para habilitar un uso que facilite sustituir los elementos analógicos por los digitales, la coordinación del capital humano, los medios

financieros y auxiliarse de todos los medios tecnológicos que ayuden a ser más eficiente la administración de justicia [23].

Son varios los beneficios de incorporar las TIC en la administración de justicia, por ejemplo: un sistema judicial más eficiente gracias a la reducción de los costos de transacción; un sistema judicial efectivo gracias a la reducción de la duración de los procesos, lo cual implica ahorros de tiempo, dinero y trabajo; la administración de justicia puede ofrecer mayor información y transparencia sobre su funcionamiento; facilitar el acceso a la justicia por parte de los ciudadanos, en especial determinados colectivos tales como: los inmigrantes, personas con bajo nivel cultural, personas con discapacidad, entre otros [4], [19], [24]-[26].

Algunos autores consideran que el uso de las TIC en el sistema judicial puede darse en los siguientes ámbitos: (i) como apoyo a la gestión del proceso, es decir, facilitar el almacenamiento y búsqueda con agilidad tanto de la información jurídica como de todos y cada uno de los documentos soporte como fallos, sentencias, resoluciones, entre otros, y de las evidencias; (ii) en la fase decisoria, en la que las TIC son un soporte para que los jueces puedan tomar sus decisiones [18], [23].

En línea con los ámbitos señalados, en el caso colombiano, y siguiendo las pautas expresadas en el Código General del Proceso Ley 1564 de 2012 [27] —el cual regula la actividad procesal en asuntos civiles, de familia, agrarios y comerciales y de otras jurisdicciones cuando en estas surjan vacíos siempre que no riña con sus principios rectores—, un proceso judicial de manera general está constituido por las siguientes etapas: presentación de la demanda, admisión, inadmisión y/o rechazo de la demanda; contestación de la demanda, audiencias y diligencias; decreto y práctica de pruebas; alegatos, sentencia. Por su parte, en el Código de Procedimiento Penal Ley 906 de 2004, un proceso judicial, en general, comprende las siguientes grandes etapas: noticia criminal, denuncia, indagación e investigación y ejecución de sentencia.

A partir de lo anterior, las grandes etapas de un proceso judicial para esta investigación son: (i) gestión del proceso judicial, que comprenderá aspectos como la recepción de la demanda, entendida como la solicitud de inicio de un proceso judicial ante autoridad jurisdiccional competente; también implica las audiencias y diligencias que corresponde a las que se realizan dentro de un proceso, en la cual la autoridad judicial oye a los sujetos procesales; (ii) pruebas o evidencias, que se refieren a los elementos de convicción aportados dentro de un proceso judicial; (iii) sentencia corresponde a la decisión de la autoridad judicial basada en su criterio y en derecho; y, (iv) ejecución de sentencia, entendida como la ejecución de la sanción penal o civil impuesta mediante sentencia ejecutoriada.

3. Ciberseguridad y el marco de ciberseguridad NIST

En la literatura se encuentran varias definiciones de ciberseguridad, sin embargo, entre las más conocidas se destacan:

- La Unión Internacional de Telecomunicaciones (UIT) la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad [28].

- Conforme a la norma ISO/IEC 27032:2012 se señala que la ciberseguridad se trata de la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo, a su vez, ciberespacio como el entorno complejo resultante de la interacción de personas, *software* y servicios en internet, a través de dispositivos tecnológicos y redes conectadas a él, que no existen en ninguna forma física [29].

Por su parte, el Gobierno colombiano, en documento del Consejo Nacional de Política Económica y Social CONPES- 3854 de 2016 y en documento CONPES 3995 de 2020, define la ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales [30], [31].

Ahora bien, al conjunto de estándares, directrices y mejores prácticas para gestionar los riesgos relacionados con la ciberseguridad se le denomina marco de ciberseguridad.

Entre los más reconocidos y adoptados con mayor frecuencia están: los estándares ISO/IEC 27001/27002, seguido del estándar PCI DSS (Payment Card Industry Data Security Standard), el CIS Critical Security Controls, el marco para la ciberseguridad NIST y las diferentes versiones de la "Guía estratégica nacional de ciberseguridad" de la UIT.

El marco para la ciberseguridad NIST, cuya primera versión se lanzó en 2014, se actualizó en 2018 y se basó en el marco CIS, COBIT y la ISO/IEC 27001. Se caracteriza por considerar la ciberseguridad como un ciclo de proceso evolutivo que permite obtener una mejora continua en las organizaciones alrededor del tema de ciberseguridad. Según el estudio de Dimensional Research, en 2016 [32], el cual incluyó 300 profesionales de seguridad en TI de los Estados Unidos, el 70 % de ellos considera el marco de ciberseguridad NIST como una buena práctica.

Este marco de ciberseguridad consta de 5 funciones, con 23 categorías y 108 subcategorías. Las 5 funciones, que apoyan a las organizaciones en la toma de decisiones frente a la gestión del riesgo, son [33]:

- Identificar: determina los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.
- Proteger: desarrolla e implementa las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.
- Detectar: descubre oportunamente la ocurrencia de incidentes cibernéticos.
- Responder: define y despliega las actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.
- Recuperar: despliega las actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

4. Método

Con el fin de dar respuesta a la pregunta de investigación, se realizó una revisión de literatura y análisis documental siguiendo el procedimiento propuesto en [34], autor que amplía el planteamiento de Kitchenham *et al*. [35]. Dicho procedimiento involucra tres fases: planificación, búsqueda de información y análisis.

4.1. Fase de planificación

Se definieron las siguientes preguntas orientadoras:

PO1: ¿Por qué es importante considerar la ciberseguridad en la justicia digital?

PO2: ¿Cuáles son las TIC que se usan, los riesgos cibernéticos y las recomendaciones para cada una de las diferentes etapas de un proceso judicial?

PO3: ¿Cuáles son las funciones y categorías del marco de ciberseguridad NIST de manera general y a la luz de las etapas de un proceso judicial?

PO4: ¿Cuál es el panorama de la justicia digital especialmente en Latinoamérica y en Colombia?

Como criterios de inclusión y exclusión, se consideraron documentos publicados entre el año 2015 y el 2020, que debían responder al menos 1 de las 4 preguntas orientadoras; el idioma de las publicaciones podría ser inglés, castellano, portugués, italiano y francés. Además, se utilizó la estrategia de bola de nieve para incluir aquellos documentos que eran citados y que dan respuesta a las preguntas orientadoras, sin importar si estaban o no en el periodo inicialmente definido. Vale la pena aclarar que los documentos a los que se accedieron son aquellos que se obtienen gracias a la suscripción de las universidades, sin que esto implique un pago adicional.

4.2. Fase de búsqueda

Se definió una estrategia de búsqueda de información de artículos y documentos académicos indexados en las bases de datos: JSTOR, Scopus, ACM y Scielo. También, se definió otra estrategia de búsqueda de información no estructurada. Ambas estrategias incluyeron palabras clave en español y en inglés como *cybersecurity*, *justice*, "*judicial system*", "*criminal justice*", *cyberjustice*, "*judicial process*", *e-justice*, "*digital justice*".

4.3. Fase de análisis de los hallazgos obtenidos

Una vez aplicadas las estrategias de búsqueda, se obtuvieron un total de 1098 documentos. Al aplicar los criterios de inclusión y exclusión y la estrategia de bola de nieve, se seleccionaron un total de 110 documentos para leer en profundidad, los cuales se clasificaron según las etapas de un proceso judicial y las funciones y categorías de la NIST, antes mencionadas.

Posteriormente, utilizando el *software* VoSViewer, se realizó un análisis de coocurrencia de las palabras clave; en la siguiente sección se presentan los hallazgos.

5. Resultados

5.1. Descripción general de los documentos

El conjunto de 110 documentos estaba conformado por 36 artículos de revista, 23 informes, 5 libros, 19 capítulos de libros, 12 artículos presentados en conferencias, 9 normas o leyes y 6 tesis.

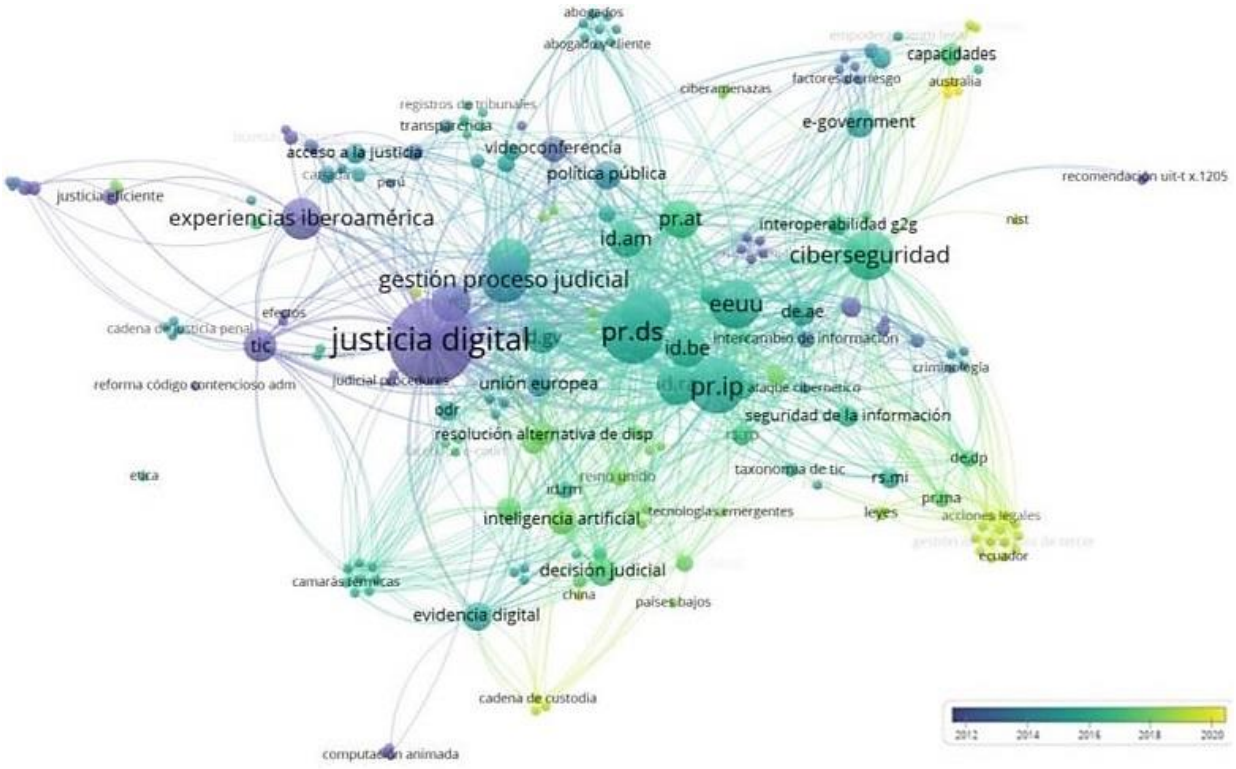
Igualmente, se encontró que 73 documentos describen casos, de los cuales 30 se desarrollan en Norteamérica, 24 en Estados Unidos y 6 en Canadá; 25 están relacionados con Latinoamérica: Argentina, Brasil, Colombia, Costa Rica, El Salvador, México, Perú, Venezuela; 12 son de Europa: Francia, Finlandia, Holanda, Noruega, Reino Unido; 5 son de Asia: China, India, Jordania y Malasia; y uno de África en Cabo Verde.

El análisis de co-ocurrencia de palabras clave presentado en la figura 1 muestra tres conjuntos de documentos a lo largo del tiempo: un primer conjunto con documentos, fechados entre 1995 y 2013, que describe las bases conceptuales de la justicia digital, identificados en color morado; un segundo conjunto de documentos, publicados entre 2014 y 2018, que presenta los riesgos cibernéticos y las funciones del marco de ciberseguridad NIST (en color verde); y un último conjunto de documentos, en color amarillo, donde se presentan técnicas computacionales disruptivas como la inteligencia artificial; estos fueron publicados en 2019 y lo que va corrido de 2020.

5.2. Descripción general de los documentos

De acuerdo con los hallazgos, son varias las razones para considerar la ciberseguridad en la justicia digital: en primer lugar, es importante tener presente que la separación entre los poderes ejecutivo, legislativo y judicial es la piedra angular de los países democráticos.

En ese sentido, como señalan Rosa *et al.* en [11], los ciudadanos esperan tener un sistema de justicia justo, eficiente y transparente, para alcanzar una mejor justicia; por lo anterior, la justicia se trata de un servicio básico e imprescindible.



Nota: Seguridad de los datos (PR.DS), procesos y procedimientos de protección de la información (PR.IP), evaluación de riesgos (ID.RA), gestión de identidad, autenticación y control de acceso (PR.AC), estrategia de gestión de riesgos (ID.RM), entorno empresarial (ID.BE), gobernanza (ID.GV), planificación de la respuesta (RS.RP) y anomalías y eventos (DE.AE).

Figura 1. Análisis de co-ocurrencia de palabras y su agrupación en el tiempo. Fuente: elaboración propia usando el *software* VoSViewer.

Por ello, la justicia hace parte de los sectores considerados como infraestructuras críticas que son esenciales para el mantenimiento de las funciones sociales, y la interrupción o destrucción de estas tendría graves consecuencias [3].

En segundo lugar, la justicia digital, además de manejar los datos confidenciales de los litigantes, tales como los números de identificación de personas naturales y jurídicas, números de cuentas bancarias, información de la víctima en casos de violencia doméstica y agresión sexual, archivos de la jurisdicción de familia que involucran a niños y familias; informes médicos y psicológicos; testimonios dentro de transcripciones y grabaciones selladas; propiedad intelectual y secretos comerciales; registros de deliberación judicial; datos de los servidores judiciales, datos financieros del sistema judicial, entre otros, que se constituyen en información sensible, puede contener información confidencial del Gobierno relacionada con la seguridad nacional. Por ello, se requiere que el umbral de protección de datos sea mucho más alto y se refuerza el concepto de infraestructura crítica [36]-[38].

En tercer lugar, cuando la prestación del servicio de justicia se realiza mediado por las TIC, pese a la especificidad del sistema judicial, no es muy diferente del uso de las TIC por parte de las instituciones financieras, las empresas, las pymes, u otras entidades estatales. Sin embargo, por su responsabilidad pública, convierte al sistema judicial en un objetivo para los cibercriminales [37]; como lo señalan Ganesin *et al*. en [39] y Pijnenburg-Muller en [40], la ciberseguridad debe ser contemplada en todas las áreas de la sociedad: judicial, social y económica, en especial para los países en desarrollo.

En último lugar, los datos judiciales son valiosos para los ciberdelincuentes, en la medida en que la información podría ser utilizada para propósitos criminales, pues estos pueden querer secuestrar este tipo de datos y pedir por el pago del rescate, como ocurrió en el Tribunal de Menores del Condado de Columbia, en la oficina del secretario del circuito en Ohio y en la Rama Judicial en Minnesota, en Estados Unidos en 2017 [37]. El costo de la pérdida o robo de información sensible es un serio problema [41].

De otro lado, el acceso a los sistemas judiciales podría permitir a los ciberdelincuentes manipular los registros de datos judiciales, poniendo en peligro la credibilidad del proceso judicial. Además, las violaciones a la privacidad de los datos pueden detener las operaciones judiciales a medida que se ejecutan las medidas de respuesta [37].

5.3. TIC, riesgos cibernéticos y las recomendaciones para afrontarlos según las etapas de un proceso judicial

A continuación, se describirán las TIC, los riesgos cibernéticos que ellas conllevan y las recomendaciones para afrontarlos en cada una de las etapas del proceso judicial digital.

5.3.1. Etapa de gestión del proceso

En la etapa de la gestión del proceso judicial, se encontró que entre las TIC más mencionadas están: los sistemas de información, las videoconferencias y los *online dispute resolution* (ODR por sus siglas en inglés). Los sistemas de información son el medio por el cual se automatizan los procesos que contienen tareas reiterativas y permiten capturar, analizar y comunicar la información asociada al expediente judicial para la operación de los procesos [11], [42]. También, se encuentran las bases de datos jurisprudenciales, accesibles vía portales [12], [20].

El almacenamiento, análisis y comunicación de la información dan lugar al uso de otras TIC como las redes, los servidores y el almacenamiento en la nube. A lo anterior, se suma el uso de portátiles, *tablets*, teléfonos inteligentes, que los servidores judiciales pueden usar para avanzar en sus tareas. El uso de sistemas de información trae múltiples beneficios, entre otros, están el incremento de la efectividad del sistema judicial, la disponibilidad de la información en tiempo real tanto para los usuarios como para los servidores judiciales y la reducción de tiempos. Sin embargo, se presenta como riesgo el confiar demasiado en el sistema de información, evitando asumir responsabilidades relacionadas con los deberes de los servidores judiciales. Los sistemas de información son una herramienta para ayudar con el trabajo, para realizar sus tareas, pero no reemplazan la intervención humana [11].

Por su parte, las videoconferencias no son nuevas en el sistema judicial, como lo señala Bellone [43], en Estados Unidos se han utilizado desde 1970. La videoconferencia es una tecnología interactiva que transmite datos de audio, vídeo y otro tipo para que dos o más partes puedan comunicarse entre sí [44], [45]. En otras palabras, lo anterior da lugar a las audiencias virtuales, las cuales pueden definirse como la utilización de los medios técnicos para la presencia virtual de personas, lo cual permite disponer desde otro sitio de las personas requeridas para adelantar diligencias en los procesos judiciales [46].

La mayoría de los países desarrollados —incluidos Australia, Canadá, Reino Unido, Singapur—, desde hace tiempo hacen uso intensivo de las videoconferencias en los procesos judiciales [47].

Varios autores como Amoni Reverón [48], Bellone [43], Davis *et al.* [44] concuerdan que es vital que estas sean de alta calidad técnica en la conexión para que la comunicación sea fluida, sin interrupciones, en las que se permita que el juez y los demás sujetos procesales se observen y escuchen con detalle, al mismo momento en que se producen sus manifestaciones, como si estuvieran uno frente al otro.

Entre los beneficios que las videoconferencias traen para los procesos judiciales están: el incremento de la versatilidad y la facilidad en la gestión, la ampliación del acceso a la justicia por parte de la ciudadanía dada la posibilidad de acceder desde diferentes lugares sin desplazamientos, el aumento de la seguridad en la medida en que se evitan los desplazamientos de cierto tipo de individuos de la población privada de la libertad; asimismo, se facilita la mediación de informes de expertos al no incurrir en los costos de tiempo y dinero generado por los desplazamientos; se plantea una innegable posibilidad de incremento en la capacidad de respuesta efectiva a necesidades del sector justicia y su acción interinstitucional [17], [43], [47], [49].

Entre las preocupaciones de usar las videoconferencias están [43], [44], [48]: i) los problemas técnicos por fallos de la tecnología, los cuales pueden frustrar a jueces, magistrados, abogados y clientes. Los retrasos entre audio y visual son molestos. Las cámaras causan dificultades, pues las personas actúan de manera diferente frente a ellas. ii) Las dificultades técnicas pueden afectar la capacidad del acusado de confrontar a testigos en su contra o reprimir la evaluación de un investigador de la confiabilidad de un testigo. Esta evaluación puede hacer que la videoconferencia sea particularmente inadecuada para situaciones en las que un testigo tiene problemas para hablar con claridad o aprendió inglés como segundo idioma. iii) Las audiencias de baja calidad por videoconferencia pueden tener un efecto perjudicial en la medida en que pueden conllevar a percepción de injusticia. Y iv) la confianza entre el abogado defensor y su cliente puede perderse, subyace la pregunta de si es igual de efectiva como con el proceso cara a cara.

Por otra parte, los ODR son mecanismos alternativos para resolución de conflictos, tales como la mediación, el arbitraje, la facilitación de diálogo, etc., a través de las TIC, en los cuales no intervienen los jueces, donde suelen resolverse conflictos de pequeñas cuantías que evitan sobrecargar el sistema judicial [38], [50]. En consecuencia, los ODR permiten el procesamiento rápido de la información y reducir los tiempos de desplazamientos disminuyendo las barreras de acceso a la justicia y las diferentes jurisdicciones, con lo que se amplía la cobertura, muy especialmente, si se da la posibilidad de usar una red social como Facebook, como mecanismos alternativos [24], [50].

Los sistemas judiciales estatales son guardianes de los datos confidenciales para individuos y organizaciones. Cuando se trata de activos de datos digitales, los sistemas de los tribunales estatales no son diferentes a las instituciones financieras, las empresas minoristas, los proveedores de atención médica y otras organizaciones gubernamentales. Esta extraordinaria responsabilidad pública los convierte en un objetivo de alto valor para los cibercriminales [37].

En ese sentido, se identificaron varios riesgos cibernéticos asociados a las TIC que se involucran a esta etapa del proceso judicial digital, entre ellos están:

- Alteración de la información cuando se realizan cambios en el contenido de una base de datos o se adicionan registros, sin importar que las bases de datos o los sistemas de información se encuentren o*n-premises* o en cualquiera de las modalidades de almacenamiento en la nube [11], [51].
- Ataques avanzados de amenazas persistentes o *advanced persistent threat* (APT) y ataques de inyección de código (ACI): los APT intentan mantener el acceso continuo y extendido a una red reescribiendo continuamente códigos maliciosos (*malware)* y utilizando técnicas sofisticadas de evasión. Un ataque APT exitoso resulta en un control invisible completo de los sistemas de información durante un período de tiempo prolongado. Por su parte, los ataques de inyección de código implican el envío de código incorrecto a los sistemas de información o a las bases de datos. A través de estos ataques, los ciberdelincuentes engañan al sistema objetivo para que ejecute un comando o permita el acceso a datos no autorizados. El ataque de inyección de código más común utiliza el lenguaje de consulta estándar a bases de datos (SQL), aunque también se encuentra en consultas LDAP, Xpath o NoSQL; comandos del sistema operativo; analizadores sintácticos de XML; cabeceras SMTP; parámetros de funciones, entre otros [37].

- Fallos en la seguridad de la información: Una preocupación natural de las partes es que revele la información que se usa en un proceso judicial, por tanto, debe asegurarse de que solo se use para un propósito específico y no se divulgue o acceda innecesariamente, preocupación que se agrava cuando se almacena y transmite electrónicamente; máxime cuando el propósito de un ciberataque es obtener información clasificada y sensible para ganar una ventaja y realizar daños en infraestructura crítica [41], [52], [53].
- Fallos en los intercambios de información: este riesgo está asociado con los problemas de intercambio de información entre los participantes de los procesos judiciales, incluidos los jueces que obtienen información sobre los procesados o los abogados que obtienen acceso completo a los archivos [54].
- Hackeo de las sesiones de videoconferencias para sabotaje, puede darse por personas externas cuando se quiere hacer daño a la infraestructura crítica relacionada con la justicia o puede darse por parte de los sujetos procesales [55].
- *Phishing:* utiliza la ingeniería social para solicitar información personal de usuarios desprevenidos para comprometer sus propios sistemas. Los correos electrónicos de *phishing* parecen legítimos y manipulan a los usuarios para que ingresen elementos como nombres de usuario o contraseñas, que pueden usarse para comprometer las cuentas. El *spear-phishing*, un método más personalizado, podría apuntar a jueces y empleados judiciales específicos [37].
- *Ransomware* infecta el *software* y bloquea el acceso de una organización a sus datos hasta que se paga un rescate. A través de correos electrónicos de *phishing*, descargas automáticas y vulnerabilidades de *software* sin parches, los ciberdelincuentes intentan extorsionar a los usuarios encriptando sus datos hasta que se cumplan ciertas condiciones. El resultado es una pérdida de datos temporal o incluso permanente. La posibilidad de robo de información asociada al proceso judicial afecta la credibilidad en el mismo [37], [56].
- Robo de información biométrica relacionados con la voz y visualización de rostros durante las audiencias virtuales [55].
- Violación de la privacidad en el contexto de la publicación de los procesos judiciales digitales: La mayor accesibilidad a los informes legales que pueden ofrecer las TIC significa que cualquier información personal contenida en el informe del proceso puede obtenerse más fácilmente. Además, es importante que exista algún método por el cual se pueda determinar de manera confiable el autor de un documento electrónico. En particular, para que una comunicación se base en ella, debe ser posible demostrar con un alto grado de certeza que un documento no ha sido alterado de ninguna manera [52]. Este riesgo también surge cuando se usan los ODR mediante redes sociales como Facebook: la información que allí se comparta se convierte en un tema público [24].

Entre las recomendaciones para mitigar los posibles ataques que se encontraron están: para proteger la información, el sistema judicial debe enfrentarse con una mayor coordinación interna y colaboración entre los juzgados y tribunales. A través de este proceso, los tribunales pueden establecer un marco de gobernanza de datos que, por una parte, proteja la privacidad de todos los involucrados en el proceso judicial [37], [57] y, de otra, le dé mecanismos a la administración de justicia para sacar provecho de esa información y ser eficiente [58]. Es conveniente, para apoyar la protección, la inclusión de mecanismos como las firmas digitales, el archivo seguro de documentos digitales y el estampado cronológico de mensajes de datos, entre otros [59].

Es necesario establecer qué información de los procesos judiciales digitales realmente se debe compartir con el público. Para ello, se requiere que la información sea clasificada [60] y diseñar los sistemas de información con el principio de "minimizar" la cantidad de información personal que procesa.

Desde una perspectiva de ciberseguridad, la estrategia de minimizar puede contribuir a reducir el área de impacto de las violaciones de datos resultantes de ataques cibernéticos o incidentes [61]. Se debe tener en mente el enfoque de protección de datos "por diseño", que se refiere a la adopción de soluciones técnicas, tecnológicas u organizativas relevantes y *ad hoc* que refuercen la privacidad en las especificaciones de diseño y la arquitectura de sistemas y procesos. Otra opción es el diseño de los sistemas de información con métodos ágiles que rápidamente podrían mostrar las debilidades de un sistema [62].

Un camino, que es subvalorado por los especialistas de ciberseguridad, es promover la cultura de la privacidad y la protección de los datos personales, tanto en las organizaciones como en los individuos.

Como lo señala Bonfanti, en [61], el reto es que los sujetos procesales junto con los jueces y los abogados tengan la capacidad de proteger directa o indirectamente el ciberespacio, donde se mueve la información jurídica. Algo no menor, desde la perspectiva, implica que hay respeto por ello y que se requiere regulación.

Aunado a lo anterior, se requiere trabajar en disminuir la carencia de habilidades informáticas genéricas y específicas de los usuarios internos del sistema judicial como de los ciudadanos en general [11]. Máxime si se considera que, según Devoe y Frattaroli [47], a los abogados y servidores judiciales les toma tiempo adoptar la tecnología por ser muy conservadores, por ello, es necesario la capacitación de manera continua.

Para disminuir los riesgos por el uso de la videoconferencia en los tribunales, Bellone, en [43], aclara que es importante que se actualicen continuamente los equipos de videoconferencia, se establezcan procedimientos de estandarización para el uso de videoconferencia y se limite el uso de las videoconferencias a diligencias judiciales. El mismo autor sugiere que se capacite continuamente a los servidores judiciales, no solo en los aspectos técnicos del uso de los equipos de videoconferencia, sino en las estrategias para generar confianza y entendimiento entre los sujetos procesales.

Es necesario ser conscientes que existen elementos facilitadores e inhibidores para compartir información entre agencias estatales. Entre los facilitadores están la capacidad de infraestructura tecnológica, la seguridad y privacidad de la información, las lecciones aprendidas de otros proyectos, la confianza, el conocimiento de la entidad, la voluntad política de las entidades y los beneficios percibidos. También, es importante diagnosticar las capacidades de intercambio de información en el sector justicia para apoyar la toma eficaz y eficiente de decisiones, incluido el análisis de delitos en tiempo real [63].

Por su parte, en los inhibidores se encuentran la capacidad del personal de TI, la confianza entre las entidades, el financiamiento y el cumplimiento de la normatividad [64]-[66]. También, Banks *et al*. [67] recomiendan compartir más información entre los tribunales para que los datos no puedan "pasar por alto" entre las jurisdicciones y para desarrollar formatos de consenso para los datos digitales utilizados en los tribunales y, así, evitar problemas de incompatibilidad.

Para asegurar que la información sea confiable, es importante el uso de estándares y la capacitación para garantizar que los datos se capturen de manera adecuada y precisa [11].

Para garantizar el acceso controlado a los sistemas de información, [68] recuerda aspectos como la responsabilidad por parte del personal de tecnologías de la información de la protección de sus cuentas como administradores. Dado que la mayoría de los delincuentes usan las cuentas de otros para sus ataques, las organizaciones podrían implementar la autenticación multifactor en sus entornos; esto implica usar más que un nombre de usuario y contraseña para acceder, los escaneos biológicos y las contraseñas únicas enviadas como mensajes de texto a teléfonos celulares son algunos ejemplos, y, por último, no olvidar incrementar la detección de riesgos a través del monitoreo de los *logs* de actividades.

5.3.2. Etapa de presentación de pruebas o evidencias

Cuando la evidencia electrónica empezó a ingresar, el sistema judicial se enfrentó a la tarea de evaluar la admisibilidad de dicha evidencia, la cual hoy afortunadamente es aceptada [69], [70]. La evidencia digital para el estudio de los casos, sin importar la jurisdicción, tiene múltiples orígenes.

Por ello, se identificó que las fuentes más comunes de evidencia son los correos electrónicos, audios y videos [71], [72]. Por otra parte, también se identificó que otras fuentes menos comunes son el uso de simuladores computacionales y el uso de realidad virtual, que llevan tiempo siendo contemplados [73]. En Estados Unidos es usual que a través del modelado holográfico virtual en 3D o animaciones forenses se recreen las escenas del crimen, a partir de la opinión de los sujetos procesales, lo cual permite aclarar a todas las partes los hechos, promover la solución pronta gracias a la ilustración de los casos y convencer con argumentos a quienes toman la decisión [73], [74].

También se encontró que la evidencia puede ser recolectada a través de drones, cámaras de video, imágenes satelitales, cámaras térmicas, dispositivos con geoposicionamiento espacial (GPS) y los nuevos dispositivos que se desarrollen gracias a la incorporación de sensores portátiles o no conectados a internet, conocido como el internet de las cosas (IoT por sus siglas en inglés) [55], [75], [76].

Por último, se encontró que, con el advenimiento del análisis de la analítica de datos, las agencias de inteligencia y de aplicación de la ley examinan rutinariamente cantidades masivas de lo que muchos consideran datos privados o personales, a través de las búsquedas en las redes sociales, los cuales también han empezado a ser consideradas como una posible fuente de evidencias [76], [77].

En general, el beneficio de estas TIC señaladas es que reducen los tiempos y los costos del proceso de aportar las evidencias [73], [76], aunque una preocupación natural es la falta o poca confianza en la tecnología y, por ello, se corre el riesgo de que algunas pruebas puedan ser inadmisibles dentro de los procesos judiciales [69], [73], [78].

Igualmente, se encontró que el uso de las anteriores TIC puede ocasionar los siguientes riesgos cibernéticos:

- Alteración de la información: dado que el principal papel de estas tecnologías es recolectar evidencia, cualquier adulteración incidiría en la decisión que posteriormente el juez tome, por ello, es importante su protección [76], [79].
- Hackeo de los dispositivos: dada la recolección de los patrones de comportamiento de individuos y organizaciones con las TIC, los *hackers* pueden usarlas para espiar o dañar a individuos u organizaciones [55].
- Robo de la información y daños a la reputación: las TIC antes mencionadas permiten recolectar información biométrica sensible, es decir, las huellas dactilares, las características de la voz, los rostros, la retina y los termogramas, por ello, es importante evitar que caigan en manos criminales [55]. Además, se encuentra el robo de información propiedad de las organizaciones; si ella es robada, puede afectar la reputación y, en consecuencia, afectar negativamente los precios de las acciones o reducir el consumo o la confianza en una organización [80].
- Violación a la privacidad: tecnologías como drones, cámaras de video, imágenes satelitales, cámaras térmicas, dispositivos con geoposicionamiento espacial y los dispositivos basados en IoT recolectan bastante información sobre los patrones de comportamiento de individuos y organizaciones, por ello, se presenta el dilema relacionado con el deber de informar a las personas filmadas, el tiempo y el contenido de las grabaciones [76]. Este riesgo también es propio de la evidencia recolectada desde las redes sociales; por eso, resalta la necesidad de una mayor educación, leyes y políticas para garantizar que estos sitios y la difusión de información estén bajo la autoridad de la Policía, al tiempo que protegen los derechos del público [76], [77].

Las recomendaciones que se encontraron son: primero, es imperante el cuidado y la protección de las evidencias de los procesos, no solo las que *per se* son digitales, sino del proceso de conversión de las evidencias análogas a digitales para evitar las brechas "decisionales" que pueden existir entre quien colecta la evidencia y quien la usa para la toma de decisiones [75], [78]; segundo, el sistema judicial debe tratar grandes cantidades de datos, volumen que crece día a día, por lo que debe tener las capacidades de talento humano y recursos financieros y de infraestructura necesarios para manejar ese volumen de datos [81], [82].

5.3.3. Etapa de decisión judicial

En la etapa de la decisión judicial, se observó que entre las TIC que se usan, además de las ya señaladas en las otras etapas, están los sistemas basados en técnicas computacionales de minería de textos, de analítica de datos (conocida como *legal analytics*) y de inteligencia artificial como el aprendizaje de máquina supervisado o el uso de *chatbots*.

La minería de textos, junto con el aprendizaje de máquina supervisado, ha permitido el desarrollo de sistemas predictivos que usan los textos de decisiones judiciales de casos ya juzgados, que pueden ofrecer a los abogados y jueces una herramienta útil de asistencia, en la preparación de los casos para los primeros y en la toma de la decisión judicial para los segundos [83].

Por su parte, la analítica de datos aplicada al ámbito jurídico, es decir, el procesamiento de altos volúmenes de información, combinada con el aprendizaje de máquina supervisado, han sido utilizados para desarrollar sistemas que permiten analizar miles de sentencias para: i) identificar patrones y elementos clave en casos judiciales similares al que se esté analizando como insumo para las decisiones, como es el caso de la Fiscalía en Argentina, de la Corte Constitucional en Colombia o del sistema judicial en China [84]-[86]; ii) predecir las posibles formas de decisión de un tribunal o juzgado con base en las decisiones previas en Francia, Canadá o la Corte Interamericana de Derechos Humanos [87]-[89]; iii) ayudar en la negociación y en el arbitramiento, ofreciendo diferentes posibilidades a través de los ODR como en Canadá [36], [56]; y, iv) para fijar las fianzas y sentencias basadas en el riesgo, a partir de los datos disponibles de los sujetos procesales [72].

La analítica de datos también se combina con el uso de *chatbots* basados en técnicas de inteligencia artificial, como el procesamiento de lenguaje natural y *deep learning*, que conversan en términos humanos, los cuales interactúa con abogados y jueces para orientar y brindar ideas potenciales para establecer un paralelismo entre casos y, al mismo tiempo, responder, obtener y derivar conocimientos relevantes de la enorme cantidad de datos legales [90].

Varios de estos sistemas han incursionado en el uso de computadores cuánticos para disminuir los procesamientos y apoyar los procesos de decisión [91].

Los beneficios de usar estas técnicas computacionales se reflejan en que reducen sustancialmente los tiempos de análisis de datos, por parte tanto de los sistemas de información usuales como de los servidores judiciales involucrados [56], [84]. Sin embargo, existen preocupaciones propias del uso de la inteligencia artificial, en la medida en que existe la posibilidad de que se den sesgos, cuando los sistemas están aprendiendo, en detrimento de ciertas poblaciones [56]. También hay otras preocupaciones propias del uso de la inteligencia artificial, relacionadas con la propiedad intelectual digital, el cumplimiento de los derechos humanos y la ética [85]. Algunos consideran que el uso de las TIC en la etapa de decisión judicial tiene como riesgo que los juzgadores podrían quedar definitivamente aislados y privados de toda capacidad de influencia en el proceso judicial [18].

El análisis identificó varios riesgos cibernéticos asociados a las TIC que se involucran en la etapa de decisión judicial, entre ellos están [85]: alteración de la información, robo de la información del proceso, robo de información sensible y violación de la privacidad, a medida que se revele información de las decisiones judiciales antes de ser proferidas.

Entre las recomendaciones para mitigar los posibles ataques que se pueden reseñar están: que los sistemas tengan acceso únicamente a los datos que son estrictamente necesarios, que no los almacene ni modifique ni realice copia de estos [84]; que los sistemas aprendan con un conjunto de datos estable que no se actualice constantemente [85].

5.3.4. Etapa de ejecución de sentencias

En la etapa de la ejecución de las sentencias, se encontró que las TIC que se usan, además de las ya señaladas en las otras etapas, son los dispositivos que cuentan con sensores como artefactos de lo que se denomina el internet de las cosas (IoT) y los sistemas de información. Así, están los sistemas de información relacionados con la gestión de los establecimientos penitenciarios y los sistemas de seguimiento a través de las pulseras y los brazaletes electrónicos, que son usados en los desplazamientos de la población privada de la libertad, o cuando se les ordena prisión domiciliaria. Estos dispositivos están en pleno auge en distintos lugares del mundo, interactúan constantemente enviando y recibiendo datos de geolocalización [55].

Otros sistemas de seguimiento están conformados por los sensores, tanto portátiles como contenidos en la infraestructura, conectados a internet, a la web semántica y a los agentes inteligentes para compartir y analizar las fuentes de datos para apoyar la ubicación y el seguimiento de los delincuentes [75].

También están los sensores biomédicos, los cuales evalúan y monitorean la salud y seguridad de los oficiales que cuidan los centros penitenciarios. Estos sensores deben controlar los niveles de estrés, fatiga y lesiones. Los datos se usan para acortar dinámicamente los turnos de trabajo, si los niveles de fatiga son excesivos [75].

Si bien, el principal beneficio del uso de los dispositivos de IoT es que hay control sobre la población privada de la libertad y facilita la gestión de los centros penitenciarios, se manifiesta la preocupación por cierta intromisión del Estado en la intimidad [55], [67], [75], [76].

También, se identificaron varios riesgos cibernéticos asociados a las TIC que se involucran en la etapa de ejecución de las sentencias, por ejemplo: i) alteración de la información, especialmente, de los sistemas de geolocalización para los privados de la libertad buscando engañar al sistema judicial [55], y de los sistemas de información para la gestión de los establecimientos penitenciarios. ii) excesivos esquemas de encriptación, pues las compañías que producen estos dispositivos IoT, en aras de dar confianza a sus usuarios, los protegen mucho mediante esquemas de encriptación, sin embargo, en China, Estados Unidos y Rusia se obliga a las compañías a que tengan un mecanismo para que la justicia pueda entrar a desencriptar la información aquí recolectada [55]. iii) hackeo de los dispositivos IoT. Si bien, el uso de tecnologías como la geolocalización para la población privada de la libertad facilita el seguimiento y la recolección de bastante información sobre los patrones de comportamiento de individuos y organizaciones, los *hackers* pueden usarlas para espiar o dañar a individuos u organizaciones o incluso hacer daño corporal a quien los use [55]. iv) Robo de información asociada a la población privada de la libertad o de información biométrica perteneciente a los oficiales de

los establecimientos penitenciarios [55]. v) Violación de la privacidad derivada del uso de las pulseras y brazaletes que constantemente recopilan y envían datos a la red y ponen en jaque la intimidad de sus dueños [76], [92].

Entre las recomendaciones para mitigar los posibles ataques, se encontró la necesidad de capacitación para los servidores judiciales de la justicia penal sobre las implicaciones de la seguridad cibernética [72], [93].

5.3.5. Etapa de ejecución de sentencias

Los riesgos más frecuentes que se encontraron en las diferentes etapas del proceso judicial digital son: alteración de la información, fallos en el intercambio de información, falta de seguridad de la información transmitida en los procesos judiciales, *ransomware*, robo de la información del proceso, robo de la información sensible y violación a la privacidad.

Por su parte, las recomendaciones halladas en el análisis documental se pueden agrupar en cuatro categorías, así:

a. Fortalecer el marco legal: se coincide con Mcmillion [94], Pijnenburg-Muller [40], Toapanta *et al*. [95] en que un marco legal adecuado es el esqueleto de la ciberseguridad, el cual permite el desarrollo de esta a largo plazo, por ejemplo, a través de herramientas que permitan judicializar y castigar a aquellos que atacan a través del ciberespacio. De acuerdo con Kramer y Butler [96], a menudo se carece en los países en desarrollo del marco legal adecuado, prueba de ello en un país como Colombia, como lo señala Sánchez-Acevedo en [97], se requiere el desarrollo de régimen jurídico para: identificación electrónica de ciudadanos, servidores públicos y sedes electrónicas; esquema de interoperabilidad de los sistemas; y para las tecnologías como la analítica y el *big data*.

b. Desarrollar programas de concientización y capacitación. Estos programas se pueden clasificar según a quienes estén dirigidos. Hay un conjunto de programas de concientización y sensibilización dirigido a los servidores judiciales, incluidos jueces y magistrados, y a los abogados en los que se traten las siguientes temáticas [11], [47], [93], [95], [98]: (i) las habilidades necesarias para la interacción con las TIC, toda vez que a los abogados y servidores judiciales les toma tiempo adoptar la tecnología por ser muy conservadores; (ii) los riesgos que se dan en el ciberespacio; (iii) la cultura de la protección de la información y de la privacidad, puesto que es importante que los sujetos procesales conozcan cómo se manejan los datos obtenidos en los procesos judiciales en concordancia con la normatividad existente para evaluar su confiabilidad y manejo y cómo este se articula a la efectiva operatividad judicial. Otro conjunto de programas de capacitación especializada dirigido al personal técnico de TI, para la gestión de la información, la gestión de riesgos de ciberseguridad a través de la implementación de marcos de ciberseguridad, lo que contribuye a incrementar la capacidad del talento humano de equipos de TI [11], [40], [94], [96]. Aunado a lo anterior, se sugiere reclutamiento de personal ya formado para evitar los costos de aprendizaje [96].

c. Incrementar la infraestructura para manejar los ciberataques: Como se mencionó antes, se recomienda, muy especialmente, el desarrollo de buenas prácticas para definir políticas y protocolos en gestión de los riesgos cibernéticos, relacionadas con el marco de ciberseguridad de la NIST en sus funciones de: identificar a través de la evaluación e identificación de riesgos; proteger asociados con la definición de controles de acceso junto con auditorías de usuarios, el otorgamiento o revocación de autorizaciones; y detectar a través del registro e identificación de incidentes y análisis de vulnerabilidades.

Para lograrlo, y partiendo de que ha habido un aumento de graves ataques informáticos e incidentes de violación de datos, se requiere de destinar partidas presupuestales amplias, que han de ser distintas a los recursos que se destinen a la gestión propia de TIC, que deben cubrir a cada institución del sistema judicial [96], [99], [100].

Se coincide con Kramer y Butler [96] y Pijnenburg-Muller [40] en cuanto a que la escasez de infraestructura para manejar los ciberataques, combinada con un mayor uso de la tecnología, es un asunto apremiante para evitar que los cibercriminales se aprovechen de la protección inadecuada, o de la falta de preparación de gobiernos e instituciones; es importante el diseño de procesos de simulación de ataques, que pueden estar a cargo de *hackers*-buenos que están dispuestos a verificar las vulnerabilidades de un sistema o de una organización a través de procesos de simulación de juegos de ataques.

Aunado al fomento de la concientización sobre la cultura de la privacidad, es importante que los sujetos procesales conozcan cómo se manejan los datos obtenidos en los procesos judiciales en concordancia con la normatividad existente, para evaluar su confiabilidad y manejo y cómo este se articula con la efectiva operatividad judicial; para esto es necesario la coordinación entre abogados, jueces y magistrados y personal de TI, a través del manejo adecuado de la información. Para ello, es necesario saber

qué información se puede compartir, qué información es confidencial o reservada, con protocolos muy claros para compartir información dentro y fuera de las instituciones involucradas [99].

d. Aprender de las experiencias de otros: Los desafíos de ciberseguridad continúan evolucionando en alcance y sofisticación, por ende, la necesidad de fortalecer la seguridad de la información de las organizaciones públicas o privadas es común, por lo que se hace necesario comprender los esfuerzos de ciberseguridad, los aprendizajes, y las mejores prácticas, por ejemplo, en la notificación de incidentes, en las herramientas, en el intercambio de información, entre otros, mediante la innovación abierta. Es decir, a través de alianzas con el sector privado o con las redes de cooperación con otras entidades públicas nacionales e internacionales [40], [96], [100]. La innovación abierta, en este caso, además permite una serie de aprendizajes que evitan perder tiempo y recursos en soluciones que pueden no ser aptas.

Incluso es válido aprender de los ciberatacantes, en la medida en que los cibercriminales son adaptativos, y, en consecuencia, el terreno cambia constantemente en el dominio cibernético, por lo que debe haber mecanismos para reconocer y ajustarse a las realidades nuevas y prevalecientes, y para incorporarlas y responder rápidamente [101].

Sin embargo, toda innovación incremental o disruptiva requiere que se reconozca el impacto de ella dentro de la cultura de las organizaciones y del talento humano que la gestiona. Se debe tener en cuenta la particularidad de cada organización, no es recomendable tomar las prácticas y replicarlas sin más. Muy especialmente, es fundamental comprender si se facilitan o afectan los valores subyacentes al sistema de justicia [102], [103].

5.4. Funciones y categorías del marco de ciberseguridad NIST

A continuación, se presenta el mapeo de las funciones y categorías de la NIST de manera global y clasificadas por las etapas de los procesos judiciales.

El mapeo de las funciones y categorías del marco de ciberseguridad de la NIST reveló que solo 61 de los documentos mencionan las funciones o sus categorías de manera directa o indirecta.

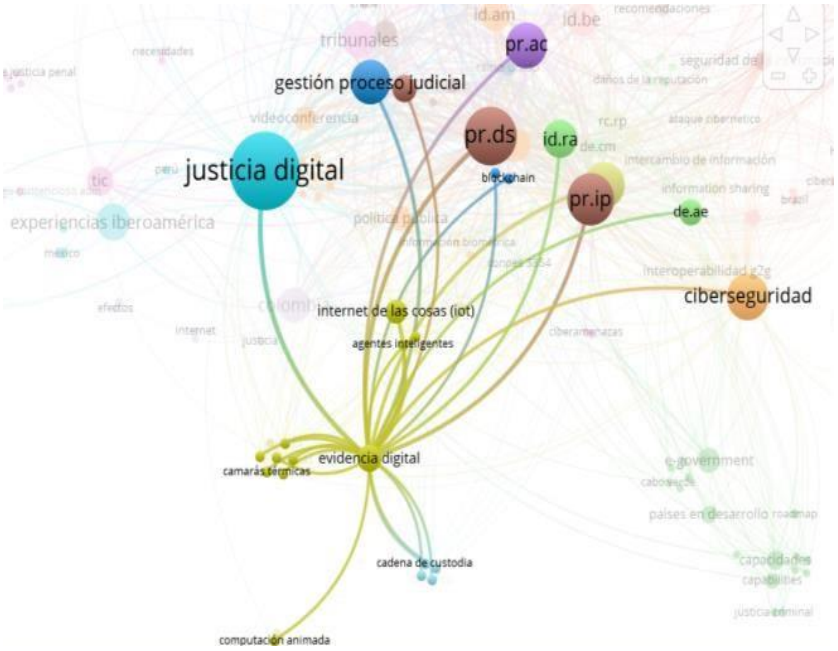
Dentro de este universo de documentos, las funciones de "proteger" y de "identificar" se destacan al ser mencionadas en un 86,89 % y 63,93 % de los documentos. Le siguen las funciones de "detectar" con un 21,3 %, "recuperar" con un 18,03 %, y "responder" con un 13,11 %.

Por su parte, el mapeo de las funciones y categorías de la NIST, con respecto a las etapas de un proceso judicial, encontró, como se observa en las figuras 2 y 3, que las categorías seguridad de los datos (PR.DS), procesos y procedimientos de protección de la información (PR.IP) y evaluación de riesgos (ID.RA) son las tres más frecuentemente mencionadas en las etapas de evidencia digital, gestión del proceso judicial y de decisión judicial. Le siguen las categorías de gestión de identidad, autenticación y control de acceso (PR.AC).

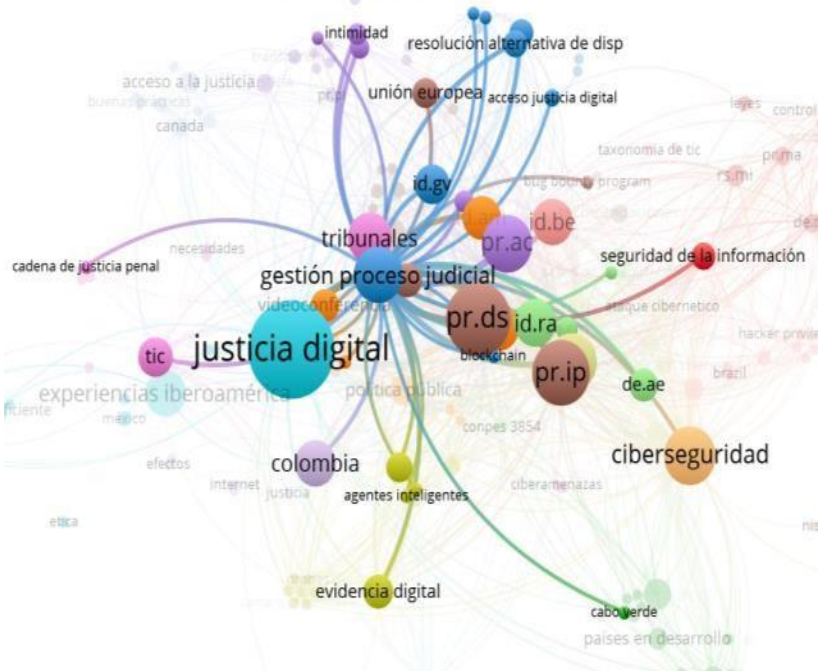
En la etapa de ejecución de la sentencia, solo se menciona la categoría de estrategia de gestión de riesgos (ID.RM) (véase la figura 3 b). En las figura 2 (b) y 3 (a) también se observa que en la etapa de gestión del proceso judicial, se destacan las categorías de entorno empresarial (ID.BE) y gobernanza (ID.GV); en la etapa de decisión judicial se destacan las categorías de planificación de la respuesta (RS.RP) y anomalías y eventos (DE.AE).

5.5. Panorama de la justicia digital, con especial énfasis en Latinoamérica

Un breve recorrido por algunos países de la región permite observar sus avances, los cuales se presentan a continuación. Como lo señala Aspis [104], la utilización de las TIC reduce la burocratización que enferma los procesos de los tribunales, tanto latinoamericanos como europeos, por ello, el desarrollo de la justicia digital es considerado un elemento clave en la modernización de los sistemas judiciales, de ahí que, desde mediados de la década de los noventa, una de las preocupaciones en el sector justicia en la región latinoamericana era desarrollar estrategias de fortalecimiento, a través del uso de las TIC, para garantizar el acceso a ella desde sitios distantes y rurales, tal y como lo señala un estudio comparado de la justicia en países de la región [105].



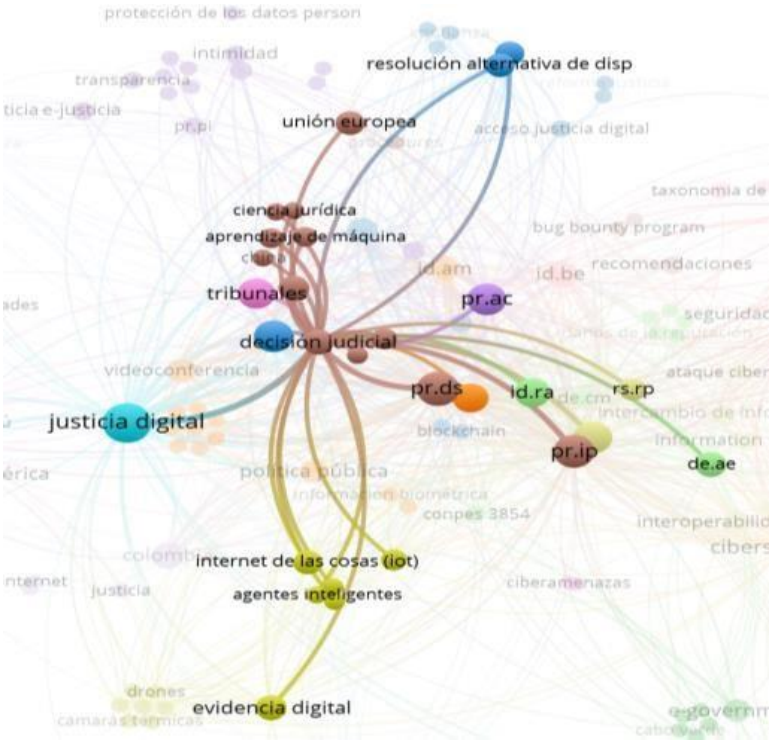
(a)



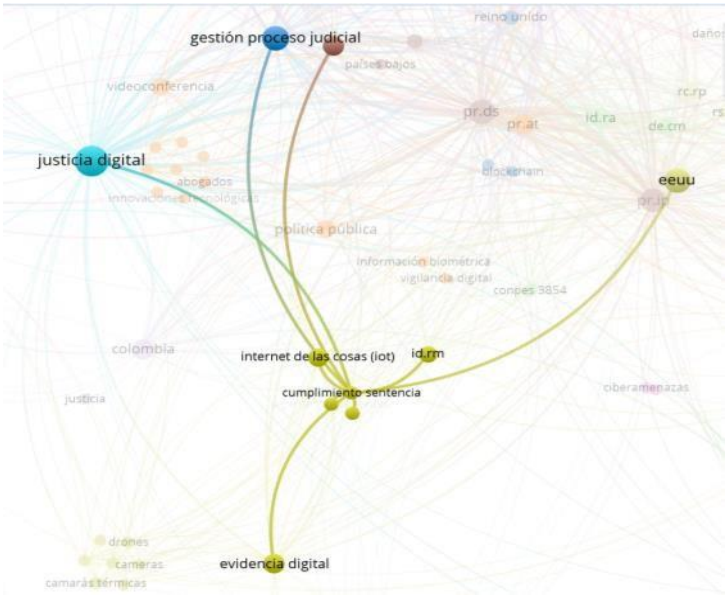
(b)

Nota: seguridad de los datos (PR.DS), procesos y procedimientos de protección de la información (PR.IP), evaluación de riesgos (ID.RA), gestión de identidad, autenticación y control de acceso (PR.AC), estrategia de gestión de riesgos (ID.RM), entorno empresarial (ID.BE), gobernanza (ID.GV), planificación de la respuesta (RS.RP) y anomalías y eventos (DE.AE).

Figura 2. Mapeo de las funciones y categorías del marco de ciberseguridad NIST en la etapa de (a) evidencia digital y (b) gestión del proceso judicial. Fuente: elaboración propia usando el método de co-ocurrencias en VoSViewer.



(a)



(b)

Nota: seguridad de los datos (PR.DS), procesos y procedimientos de protección de la información (PR.IP), evaluación de riesgos (ID.RA), gestión de identidad, autenticación y control de acceso (PR.AC), estrategia de gestión de riesgos (ID.RM), entorno empresarial (ID.BE), gobernanza (ID.GV), planificación de la respuesta (RS.RP) y anomalías y eventos (DE.AE).

Figura 3. Mapeo de las funciones y categorías del marco de ciberseguridad NIST en la etapa de (a) decisión judicial y (b) ejecución de la sentencia. Fuente: elaboración propia usando el método de co-ocurrencias en VoSViewer.

Tabla 1. Hitos de justicia digital en Latinoamérica

País	Año incursión TIC	Año de habilitación del expediente electrónico	Año de habilitación audiencias virtuales
Brasil	1951	Ley 11419 de 2006	Ley 11900 de 2009
Argentina	1990	Ley 26685 de 2011	2012
Costa Rica	1993	2008	2008
Colombia	1995	Ley 1394 de 2010. Ley 1564 de 2012, Decreto 806 de 2020.	Ley 1709 de 2014
Venezuela	2000	Decreto Ley Mensajes de Datos y Firmas Electrónicas de 2001	Código Orgánico Procesal Penal de 2012
Perú	2001	Ley 27419 de 2001	Directiva n.° 001-2014-CE-PJ, del 07 de enero del 2014
México	2009	2011	2011
El Salvador	2010	2010	2015

Fuente: elaboración propia con base en [48], [106], [107], [108], [109], [110], [111], [117], [121], [122].

Para ese entonces, 18 estados iberoamericanos ya publicaban información sobre la organización del poder judicial, normatividad, diarios oficiales y jurisprudencia a través de las TIC. Diez de aquellos países ofrecían información sobre los procesos judiciales (requisitos, procedimientos, plazos, entre otros) y sobre los servicios prestados (certificados, trámites, entre otros). También, en la mayoría de los países se facilitaba tanto el intercambio de datos entre operadores jurídicos (jueces, magistrados, funcionarios de juzgados y tribunales), como el uso de sistemas de información como apoyo a la gestión de procesos judiciales.

Así, en Argentina la implantación de las TIC en el ámbito procesal comenzó desde mediados de los años noventa, donde se incorporaron el uso de escáneres para digitalizar documentos, el uso de la firma digital, de notificaciones y pagos electrónicos, videoconferencia, entre otros; sin embargo, solo hasta el año 2011 surgió la Ley de Expediente Electrónico n.° 26685 para darle sustento jurídico al uso judicial de las TIC [48].

En el año 1993, el Poder Judicial de Costa Rica inicia el proceso de modernización. Desde el año 2000 se han venido realizando avances significativos tanto en cobertura nacional de las herramientas tecnológicas, como en el desarrollo de nuevas y mejores formas de gestión judicial, implementando, además, una gama de servicios electrónicos orientados hacia el usuario [106].

En la República Bolivariana de Venezuela, desde 2000, la Sala Constitucional, mediante sentencia 656 de 2000, estableció la necesidad de adaptar el ordenamiento jurídico a las nuevas realidades sociales, es decir, en un entorno virtual, desde la óptica técnica y jurídica, los escritos pueden redactarse, firmarse, remitirse al tribunal y archivarse en formato electrónico, ya que así lo autoriza el decreto ley sobre mensajes de datos y firmas electrónicas de 2001, a pesar de la inexistencia de una regulación especial para tal fin [48]. Ahora bien, en Venezuela, no hay regulación explícita que permita el uso de videoconferencias en el sistema judicial; sin embargo, la Ley Orgánica contra la Delincuencia Organizada y el Financiamiento del Terrorismo de 2012 contempla el uso de la videoconferencia cuando no sea posible o conveniente la comparecencia de una persona para un proceso que se esté desarrollando en otro estado; el código orgánico procesal penal de 2012 permite las notificaciones electrónicas, incluyendo aquellas que se realizan por videoconferencias; y la ley orgánica del tribunal supremo de justicia de 2010 da la posibilidad del empleo de cualquier tipo de TIC en los procesos judiciales que se lleven a cabo ante él [48].

En Brasil, en 2006, a través de la Ley 11419 se aprobó el uso del expediente electrónico que se aplica en todo tipo de procedimientos judiciales, laborales y administrativos. Sin embargo, otras TIC habían sido incluidas desde 1951. Posteriormente, mediante la Ley 11900 de 2009, se autorizó el uso excepcional de la videoconferencia en los procesos penales, para el interrogatorio de los procesados privados de la libertad [48], [109].

En México, en 2009, a través de una serie de reformas a la ley Federal de Procedimiento Contencioso Administrativo se dio origen al sistema de justicia en línea, el cual a partir de 2011 permite substanciar en todas sus partes un procedimiento jurisdiccional [110].

En El Salvador, en el año 2015, la Asamblea Legislativa aprobó la realización de audiencias virtuales a procesados por el sistema de justicia, con el fin de no interrumpir procesos penales. Está dirigida muy especialmente para la población privada de la libertad y tiene como objetivo obtener eficacia y rapidez en los procesos penales. Las primeras audiencias se iniciaron en 2016, aunque han presentado varios problemas relacionados con la falta de infraestructura y capacitación de los servidores judiciales [111].

Como se ha podido observar, los tribunales latinoamericanos han invertido tiempo y fondos nacionales en su automatización. Por lo anterior, la incorporación de las TIC para los países de la región ha constituido una oportunidad para consolidar la eficacia y eficiencia en los procesos judiciales, para estrechar un vínculo permanente del Estado con los ciudadanos, asimismo, para fomentar la participación ciudadana en los procesos judiciales y hacer transparente la información pública como arma contra la corrupción [112], [113].

Sin embargo, pese a estos esfuerzos, Beauchard [114] y Hammergren [58] coinciden en que dicha automatización no se ha utilizado para crear bases de datos mejoradas, sino para el procesamiento de textos de documentos ordinarios (documentos tradicionales escaneados), razón por la cual existe ausencia del flujo de datos sobre los casos, lo cual imposibilita evaluar los impactos.

Por su parte, en Europa, se han apoyado iniciativas de justicia digital que van desde la creación de un portal de red judicial en materia civil y mercantil, en 2003, hasta la implementación de un atlas de justicia penal y civil; todas ellas tratando de reducir la complejidad de la interacción entre la regulación, la tecnología y las organizaciones [16], [25]. De las muchas iniciativas que han visto la luz en últimos años en el campo de la justicia digital en Europa, Estados Unidos y Canadá, una de las más controversiales es el uso de los ODR [38], [50], [98].

En Canadá, los ODR han implementado el uso de la Inteligencia artificial en los procesos de decisión de los jueces, en especial, para ayudar en la negociación y la toma de decisiones, más que en su capacidad de actuar como sustituto de un abogado o un abogado o el juicio de un tomador de decisiones [56]. Por su parte, Susskind [115] sostiene que estos sistemas de tribunales en línea desplazarán a muchos litigios convencionales, y, seguramente, la inteligencia artificial, el aprendizaje automático y la realidad virtual dominarán el servicio judicial. Sin embargo, el uso de los ODR en los países en desarrollo es marginal, en general, se resuelven mejor los conflictos por presión comunitaria que mediante el acceso a los sistemas de justicia [114].

Ahora bien, en la región de Iberoamérica, el debate sobre ciberseguridad derivada del uso de las TIC en la justicia ha estado presente en las cumbres iberoamericanas de presidentes de cortes supremas y de tribunales superiores de justicia. Especial mención tiene la cumbre realizada en 2018, donde se creó una red de cooperación en materia de ciberseguridad entre los países miembros de la cumbre, con el objeto de compartir las mejores prácticas para facilitar la socialización de experiencias, evitar el desgaste de esfuerzos y fortalecer las capacidades ante las amenazas cibernéticas [116].

5.6. Panorama de la justicia digital en Colombia

Como los demás países de la región, el desarrollo de la justicia digital en Colombia también inició a mediados de los años noventa, puesto que desde 1995 se ejecutó la estrategia de sistematización del ejercicio de la función judicial y la administración de justicia, con el ánimo de adquirir equipos, desarrollar sistemas de información para la gestión de los procesos judiciales, adquirir la infraestructura de red para todos los despachos judiciales y capacitar a los servidores judiciales [117].

En 2010, a través de la Ley 1394 de 2010, que determina el arancel judicial y nutre de recursos para la descongestión judicial, se ordenó a la Sala Administrativa del Consejo Superior de la Judicatura la articulación de un plan para la inversión de estos recursos para gestionar un plan para la justicia digital. Estos esfuerzos permitieron que, para la gestión de los procesos, la Rama Judicial desarrollara *software* internamente. El primer sistema se denominó justicia XXI, el cual era cliente-servidor, y el segundo sistema se llamó justicia web, los cuales permiten la visualización de las actuaciones ordenadas por fecha, aunque de manera limitada y apoyan las estadísticas que sirven de base para la toma de decisiones, de manera básica pero exitosa [22], [118].

En 2012, el Código General del Proceso Ley 1564 de 2012 determinó el uso de las TIC en todas las actuaciones judiciales, las cuales se podrán realizar a través de mensajes de datos en la gestión y trámites de los procesos judiciales. En especial, se destaca que desde entonces se admite la evidencia digital.

Otro aspecto para destacar es que, como lo dice el Centro de Documentación Judicial, a partir de 2006 con la implementación del sistema penal acusatorio se inició la grabación de las audiencias y su posterior archivo en un *data center* que permite su consulta. El 80 % de las audiencias se generaron con el INPEC. Así, estos procesos se vieron fortalecidos con la expedición, en 2014, de la Ley 1709, la cual estableció que, en todos los establecimientos penitenciarios se deben garantizar las locaciones y elementos tecnológicos necesarios para la realización de audiencias virtuales, y de manera preferente los jueces realizarán estas audiencias. Sin embargo, los procesos de intercambio de información con otras entidades pueden dificultarse, por la poca implementación de los procesos de interoperabilidad entre las diferentes entidades del sector justicia [92], [119]. En la justicia penal se usan los dispositivos electrónicos con GPS para las detenciones domiciliarias.

En Colombia, la acción constitucional de tutela es el mecanismo más inmediato de protección de los derechos fundamentales constitucionales cuando son vulnerados o amenazados por la acción u omisión de autoridadpública, es así como a diario a los tribunales y juzgados del país llegan miles de tutelas que congestionan el sistema judicial, motivo de preocupación toda vez que, por ejemplo, en promedio entre 2015 y 2019 se recibieron 726.300 tutelas anualmente [8]. Por esto, la Corte Constitucional anunció la adopción de un programa de inteligencia artificial como iniciativa pionera de un sistema predictivo de detección inteligente de sentencias e información, llamado "Pretoria", para facilitar el trabajo de los jueces, el cual es capaz de agrupar, analizar, y clasificar información de las más de 2700 sentencias diarias que recibe la Corte [84]. Sin embargo, este es el único esfuerzo, en consecuencia, el 99 % de los despachos judiciales no usa herramientas de analítica de datos, ni tampoco minería de textos, el uso de las TIC es poco para apoyar el proceso decisional.

En los últimos tres años, es de destacar, por un lado, los planes de modernización y transformación digital como el Plan Decenal del sistema de justicia 2017-2027 y Plan Sectorial de Desarrollo Rama judicial 2019-2022 y, por el otro, el presupuesto anual del sector justicia ya que cerca de un 28 % se dedica a la inversión en TIC, lo cual demuestra que es un asunto prioritario [119].

Por último, hay que mencionar que se aceleró la justicia digital gracias al Decreto 806 de 2020, mediante el cual el Gobierno nacional, en el marco de la emergencia económica, social y ecológica por el COVID-19, adoptó medidas transitorias para el acceso a la justicia a través de medios virtuales y agilidad en los procesos judiciales, para lo cual se adopta como una de las principales medidas el uso de las TIC en los procesos judiciales [120].

Pese a estos esfuerzos, en 2020, aún no se puede hablar de un modelo de justicia en línea, debido a que los sistemas de información son solo de consulta muy global, es decir, solo se puede ver el estado del proceso y las actuaciones judiciales [118], pese a que se está construyendo el sistema de gestión judicial unificado.

También se adolece de los sistemas de información para registrar la cartilla biográfica de la población privada de la libertad, en consecuencia, los jueces que vigilan las penas no tienen acceso a ella de manera digital. Lamentablemente, tampoco existe el expediente digital único, con registro y trazabilidad segura y transparente [92]. Se espera que para 2027, conforme al Plan Decenal de Justicia 2017-2027, se haya diseñado una política de seguridad de la información y protección de datos, que incluya crear mecanismos de protección de datos, encriptación, anonimización y códigos de seguridad.

6. Recomendaciones de ciberseguridad para la justicia digital colombiana

Como se señaló, el Estado colombiano ha realizado varios esfuerzos con miras a alcanzar la justicia digital; frente a este panorama, y como se observó en el análisis de cada etapa del proceso judicial, se evidenció una serie de recomendaciones en torno a la ciberseguridad en la justicia digital, que sirven de base para las recomendaciones al caso colombiano, las cuales se presentan a continuación:

Si bien es cierto que en Colombia se ha avanzado en el marco legal para la ciberseguridad a través de diferentes políticas y mecanismos que se han venido trabajando desde el año 2011, como el CONPES 3701 sobre Lineamientos de Política para Ciberseguridad y Ciberdefensa, la Ley Estatutaria 1581 del 2012, el CONPES 3854 sobre Política Nacional de Seguridad Digital de 2016 y el Decreto 1008 de 2018, en la medida en que estas políticas y mecanismos se enfocaron en el fortalecimiento y generación de capacidades en el Gobierno nacional, para brindar confianza digital, seguridad y defensa a los ciudadanos, cabe anotar que no se ha logrado el avance esperado.

Por esta razón, se dio lugar al reciente CONPES 3995 de 2020 sobre Política Nacional de Confianza y Seguridad Nacional, que busca subsanar las falencias mencionadas al establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

En consecuencia, garantizar la confianza y seguridad digitales se constituye en un reto mayor para la justicia colombiana, que de no ser superado iría en un mayor detrimento de la credibilidad del poder judicial. La administración de justicia tiene, entonces, una responsabilidad de generar las medidas necesarias para dar celeridad y confianza a las actuaciones judiciales digitales. Por lo cual, en el marco legal se recomienda ampliar la regulación en confianza digital, al igual que se requiere el desarrollo de régimen jurídico para: i) identificación electrónica de ciudadanos, servidores públicos y sedes electrónicas; ii) esquema de interoperabilidad de los sistemas; y iii) para las tecnologías computacionales basadas en inteligencia artificial.

De otra parte, como quiera que en la Rama Judicial el personal de TI se encuentra en la Unidad de Informática, bajo la Dirección Ejecutiva de la Administración Judicial, del Consejo Superior de la Judicatura (CSJ). Allí se dispone del equipo de TI que atiende las altas cortes, los tribunales y los conglomerados de juzgados. Esa estructura se replica en las diferentes seccionales del CSJ en todo el país; ello significa que el director de la Unidad de Informática no tiene la posibilidad de asesorar directamente a quienes toman decisiones para sacar el mejor provecho de las TIC, por ello, pese a que el personal de TI esté capacitado y aplique un modelo de gobernanza de seguridad, se dificulta garantizar que la seguridad de la información sea vista como algo estratégico y relevante. Por lo anterior, sería importante que los lineamientos del Decreto 415 de 2016, que aplican a la Rama Ejecutiva, se extiendan a la Rama Judicial, de tal forma que el director de TI, quien tiene la responsabilidad al más alto nivel de las instituciones de seguridad de la información, podría establecer una comunicación constante con la alta dirección de la institución y guiarla sobre la estrategia de seguridad y protección de datos. Adicionalmente, se sugiere implementar una política pública que busque un incremento en las capacidades y en las posibilidades de responder de forma adecuada y rápida a los nuevos retos tecnológicos basados en la gobernanza digital para el fortalecimiento de la justicia en el país.

Frente al desarrollo de programas de concientización y capacitación, se considera adecuado que en el Plan Decenal del Sistema de Justicia (2017-2027) contemple un programa para fortalecer el uso y apropiación de TIC y, así, generar un cambio cultural en el sistema de justicia colombiano alrededor del uso de TIC; sin embargo, estos programas se deben complementar, como ya se indicó, con los programas de concientización y sensibilización sobre los riesgos cibernéticos, la cultura de la privacidad y protección de la información y los programas de capacitación especializada. Se recomienda la suscripción de convenios entre la Rama Judicial y el Ministerio de las TIC, para que servidores judiciales participen de las convocatorias para los varios programas de maestría en seguridad de la información, seguridad digital y ciberseguridad ofrecidos por universidades colombianas. Igualmente, es conveniente el diseño de una estrategia de formación a través de diplomados, en modalidad presencial o virtual, ofrecidos por universidades colombianas o extranjeras en ciberseguridad.

Por su parte, para incrementar la infraestructura para manejar los ciberataques, se destaca que es acertado que el Plan Decenal del Sistema de Justicia (2017-2027) proponga un objetivo específico para "generar una política de seguridad de la información y protección de datos", el cual tiene acciones concretas que se pueden relacionar con el marco de ciberseguridad NIST en sus funciones de: i) identificar mediante la detección de los riesgos de la información reservada o sensible necesaria para intercambiar a nivel interinstitucional e intersectorial, acción que debería estar terminada en 2021; ii) proteger, a través de la creación de los mecanismos de protección de datos (ejemplo: encriptación, anonimización, códigos de seguridad, entre otros), el diseño de guías y protocolos para la protección de información e infraestructura vulnerable del sistema de justicia y el análisis de puntos críticos y rutas de acción definidas, que deberían estar terminadas en 2026 y 2027; iii) detectar, por medio del fortalecimiento a nivel institucional, las áreas de tecnología y demás recursos para materializar las políticas de seguridad, junto con la implementación de procedimientos asociados a la ISO 27001, acción que se culminaría en 2023; y iv) recuperar a través de la elaboración e implementación de los planes de recuperación antidesastres de la infraestructura TIC, acción a culminar en 2026.

Sin embargo, se sugiere complementar el plan decenal con acciones relacionadas con: i) el diseño de lineamientos y protocolos para tener los suficientes controles para garantizar la confianza digital y protección de datos a los servidores judiciales, sujetos procesales y ciudadanía en general, tanto en todas las aplicaciones digitales y las herramientas de uso dentro del entorno judicial ya existentes, como en las nuevas aplicaciones que tecnologías emergentes basadas en inteligencia artificial, el uso de *chatbot*, o en dispositivos IoT pueden llegar a demandar; ii) el diseño de mecanismos que permitan reconocer, sobre toda información de los sistemas de justicia digital, quién tiene la titularidad y la autorización del manejo y el uso adecuado de esa información y, así, determinar el alcance funcional de la misma; iii) el diseño de una política de transparencia sobre cómo y para qué es tratada y usada la información

que se contempla en los procesos judiciales digitales; y iv) el diseño de un plan de pruebas de seguridad para identificar las vulnerabilidades, a través de *hackers*-buenos, y tomar las acciones necesarias para implementar controles efectivos. La ciberseguridad ha de ser una prioridad en el sistema judicial, en consecuencia, se ha de incrementar la inversión presupuestal para evitar ser vulnerable y resistir a los riesgos cibernéticos.

Para continuar aprendiendo de las experiencias de otros, es importante recordar que la ciberseguridad es compleja y requiere el compromiso y participación de expertos; se sugiere que las altas cortes sigan participando del grupo de justicia de la cumbre judicial iberoamericana, para ser parte de los diagnósticos, del análisis de brechas y del intercambio de conocimientos, que les permita generar sinergias, sin perjuicio de establecer otras alianzas que permitan generar y consolidar redes de trabajo intersectorial e interinstitucional, que busquen alinear distintos intereses de la política pública con el fin de que se consolide un efectivo crecimiento e interés en el entorno digital para beneficio de la administración de justicia desde una propuesta integradora de planes y estrategias que desarrollan construcción normativa y cambios institucionales coordinados.

También se recomienda realizar, continuamente, ejercicios como el presentado en este artículo, para estar atento a las tendencias y experiencias que los académicos y los sistemas judiciales comparten.

7. Conclusiones

Esta investigación se apoyó en una revisión sistemática de literatura que permitió identificar por qué la justicia digital es un servicio esencial que hace parte de la infraestructura crítica de las naciones, y, en consecuencia, la ciberseguridad debe contemplarse. También se identificaron las TIC, riesgos cibernéticos y recomendaciones en cada etapa del proceso judicial, lo que lleva a concluir que la ciberseguridad es un elemento indispensable en cada aspecto de la justicia digital.

Se destacan las recomendaciones basadas en el análisis de los documentos para el cumplimiento de las tareas asignadas en un rol digital, donde están asociados conocimientos y habilidades de índole tecnológicos, necesarios para mejorar la ejecución de una función de administración de justicia usando instrumentos y herramientas determinadas, que se adquieren a través del proceso continuo de utilización digital y que acarrean riesgos de la indebida utilización de estas herramientas.

El sistema judicial debe proteger la información que maneja en los diferentes procesos judiciales, en la medida en que el uso efectivo de la información dependerá de la pertinencia, accesibilidad, calidad, aprehensibilidad que se disponga; todas las acciones que se realicen en busca de esa protección colaborarán en fomentar la eficacia, eficiencia y confiabilidad de las actuaciones judiciales. De otra parte, la variedad de riesgos cibernéticos identificados en las diferentes etapas del proceso judicial demanda la gestión de estos, a través de la implementación de las funciones y categorías del marco de la NIST.

La comparación del desarrollo de la justicia digital en algunos países de América Latina deja ver que el interés por la incorporación de las TIC en la justicia se ha mantenido desde hace más de dos o tres décadas. Sin embargo, algunos países han avanzado más que otros tanto en el uso de las TIC como en el marco legal requerido.

Los hallazgos aquí presentados permiten que los servidores judiciales y profesionales jurídicos comprendan el panorama del uso de las TIC, los riesgos cibernéticos y posibles recomendaciones por etapa judicial.

Específicamente para el caso colombiano, los hallazgos de esta investigación invitan a reflexionar sobre:

a.El sector de la justicia no debería implementar las TIC únicamente por el bien que ellas causan. En cambio, es esencial una administración de justicia que le dé relevancia a la tecnología como generador de cambio, de consolidación de procesos tangibles y beneficios para el desarrollo de la sociedad que genera progreso y se enfila hacia un proceso para impulsar el Estado con procesos judiciales que sean más céleres y eficaces.

b.Es necesario implementar la gestión de las herramientas digitales como una apuesta para el fortalecimiento de la gobernanza digital y de la justicia en el país. Dicha incorporación implica considerar la gestión para mitigar los múltiples riesgos cibernéticos que pueden afectar los procesos judiciales.

c.Toda aplicación TIC está vinculada a conocimientos específicos de ejecución, de esta manera, se evidencia que la justicia digital hace referencia a grupos de prerrequisitos cognitivos, donde el sector las necesita para ser capaz de trabajar en forma adecuada en un área específica y concreta. Lo significativo es que se utilicen en la gestión diaria de las necesidades del sector, por eso, son clave dentro de una gestión acertada, ya que el

manejo de la tecnología precisa que las instituciones sean más inteligentes en la medida en que los procesos institucionales se simplifiquen y sean más céleres y eficaces, haciéndose necesario incrementar el valor de dicho conocimiento en las organizaciones del sector justicia. No debe perderse de vista que la inversión en la adquisición, desarrollo, uso y mantenimiento en TIC debe estar acompañada de una estrategia coherente de inversión en talento humano lo suficientemente calificados como para explotarlas debidamente.

d.Cómo, a partir de las recomendaciones señaladas en esta investigación, mitigar la crisis de confianza que hoy sufre la justicia colombiana, que se puede incrementar con la justicia digital por causa de una mala gestión de los riesgos cibernéticos a los que se enfrenta. El llevar a cabo estas recomendaciones puede ser un mecanismo para que los ciudadanos sientan que se les brinda una justicia digital confiable.

e.Se debe, a través de estos ejercicios, plantear una capacidad para generar y consolidar redes de trabajo intersectorial e interinstitucional que busquen alinear distintos intereses dentro del entorno digital de la política pública, con el fin de que se consolide un efectivo crecimiento de la capacidad de aplicaciones para beneficio de la administración de justicia con una propuesta integradora de planes y estrategias que desarrollen la construcción normativa y los cambios institucionales de manera coordinada.

Para finalizar, se requiere seguir investigando en justicia digital, darle la respectiva importancia a la estructura organizacional para gestionar el uso e incorporación de TIC, con la debida ciberseguridad en los procesos, y a los criterios para definir dicha estructura.

Agradecimientos

Al Ministerio de Tecnologías de la Información y las Comunicaciones, a la Escuela Superior de Guerra - General Rafael Reyes Prieto, Ministerio de Defensa. También, a la doctora Jenny Marcela Sánchez-Torres, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de esta investigación.

Referencias

[1] M. Castells, La era de la información: economía, sociedad y cultura, vol. 1. Madrid: Alianza Editorial, 1996.

[2] J. M. Sánchez-Torres, M. P. González-Zabala, y M. P. Sánchez-Muñoz, “La sociedad de la información: génesis, iniciativas, concepto y su relación con las TIC”, Revista UIS Ingenierías, vol. 11, no. 1, pp. 113-128, 2012.

[3] M. Klaver, H. Luiijf, A. Nieuwenhuijs, y E. Al, “RECIPE Good Practices Manual for CIP Policies. For policy makers in Europe”, TNO Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek 2011.

[4] A. C. Martínez, “E-justicia: las tecnologías de la información y el conocimiento al servicio de la justicia iberoamericana en el siglo XXI”, Rev. Internet, derecho y política, vol. 3, no. 4, pp. 5, 2007.

[5] S. Herbert, “Improving access to justice through information and communication technologies”, GSRDC Helpdesk Research Report 13.02.2015.

[6] L. Gordon y D. Garrie, Cybersecurity & the Courthouse: Safeguarding the Judicial Process. New York, NY, USA: Wolters Kluwer, 2020.

[7] J. Donoghue, “The rise of digital justice: courtroom technology, public participation and access to justice”, Mod. Law Rev., vol. 80, no. 6, pp. 995-1025, 2017, doi: 10.1111/1468- 2230.12053

[8] Consejo Superior de la Judicatura, Justicia Moderna con Transparencia y equidad. Bogotá, Colombia: Plan Sectorial de Desarrollo Rama judicial 2019 – 2022, 2019.

[9] Ministerio de las Tecnologías de la información y comunicaciones de Colombia, Plan Nacional de Tecnologías de la Información y las Comunicaciones 2008-2019. Bogotá, Colombia: Plan TIC Colombia, 2008.

[10] Consejo Superior de la Judicatura, Plan Decenal de Justicia 2017-2027. Bogotá, Colombia, 2017.

[11] J. Rosa, C. Teixeira, y J. Sousa Pinto, “Risk factors in e-justice information systems”, Gov. Inf. Q., vol. 30, no. 3, pp. 241-256, 2013, doi: 10.1016/j.giq.2013.02.002

[12] J. M. Sánchez-Torres, “Diseño de la metodología para la evaluación del impacto de la implementación de las TIC en la Rama Judicial Colombiana”, tesis de maestría, Universidad Nacional de Colombia, 1998.

[13] R. Heeks, "e-Government as a Carrier of Context", J. Public Policy, vol. 25, no. 1, pp. 51–74, 2005, doi: 10.1017/S0143814X05000206

[14] J. Katz y M. Hilbert, Building an information society: a latin american and caribbean perspective. ECLAC, Santiago de Chile, 2003.

[15] J. M. Sánchez-Torres, "Propuesta metodológica para evaluar las políticas públicas de promoción del e-government como campo de aplicación de la Sociedad de la información. Conceptualización y aplicación empírica en el caso colombiano", tesis doctoral, Universidad Autónoma de Madrid, 2005.

[16] M. Velicogna, "In Search of Smartness: The EU e-Justice Challenge", Informatics, vol. 4, no. 4, pp. 38, 2017, doi: 10.3390/informatics4040038

[17] I. Aaltonen, J. Laarni, y K. Tammela, "Envisioning e-Justice for Criminal Justice Chain in Finland", Electron. J. e-Government, vol. 13, no. 1, pp. 55-66, 2015.

[18] M. E. García Barrera, "Juzgado sin papel, un paso más en la justicia electrónica", Rev. IUS. Rev. del Inst. Ciencias Puebla, vol. 12, no. 41, pp. 133-154, 2018.

[19] D. Weinstock, "Cyberjustice and Ethical Perspectives of Procedural law", en eAccess to Justice, K. Benyekhlef, J. Bailey, J. Burkell, and F. Gélinas, Eds., Ottawa, Canadá: Univeristy of Ottawa Press, 2016, pp. 305-315.

[20] G. Canivet, "POSTSCRIPT: eAccess to JusticeBrief Observations", en eAccess to Justice, K. Benyekhlef, J. Bailey, J. Burkell, and F. Gélinas, Eds., Ottawa, Canadá: University of Ottawa Press - JSTOR, 2016, pp. 377-381.

[21] F. Contini y M. Velicogna, "Del acceso a la información al acceso a la justicia: diez años de e-justice en Europa", Rev. Sist. Judic., vol. 9, no. 16, pp. 30-47, 2011.

[22] R. N. Londoño-Sepulveda, "The use of ICT in judicial procedures: a proposal for online justice L'usage des TIC dans les procédures judiciaires: une proposition de la justice en ligne", Rev. Fac. Derecho y Ciencias Políticas, vol. 40, no. 112, pp. 123-142, 2010.

[23] L. Álvarez-Casallas, "Justicia electrónica", Rev. Digit. Derecho Adm., vol. 4, pp. 43-56, 2010.

[24] I. Al Swelmiyeen y A. Al-Nuemat, "Facebook e-court: Online justice for online disputes", Comput. Law Secur. Rev., vol. 33, no. 2, pp. 223-236, 2017, doi: 10.1016/j.clsr.2016.11.006

[25] Comisión Europea, "E-justice", 2010. doi: 10.1558/jsrnc.v4il.24.

[26] Pontificia Universidad Javeriana, Tecnologías al servicio de la Justicia y el Derecho. Bogotá, Colombia: Fundación Cultural Javeriana de Artes Gráficas – JAVEGRAF, 2019.

[27] Congreso de la República de Colombia, Ley 1564 de 2012, no. Julio 12. Bogotá, 2012, pp. 349–372.

[28] Unión Internacional de Telecomunicaciones UIT, "UIT-T X.1205 Aspectos generales de la ciberseguridad", Sect. Norm. Las Telecomunicaciones La Uit, vol. 1205, 2008.

[29] Information Technology-Security Techniques-Guidelines for Cybersecurity, ISO/IEC 27032:2012.

[30] Departamento Nacional de Planeación, Política Nacional de Confianza y Seguridad Digital. Bogotá, Colombia: DNP, 2020, pp. 51.

[31] Departamento Nacional de Planeación, Política de Seguridad Digital. Bogotá, Colombia: DNP, 2016, pp. 91.

[32] Dimensional Research, Trends in Security Framework Adoption. Columbia, MD, USA: Tenable network security, 2016.

[33] K. Stine, K. Quill, y G. Witte, Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, 2014.

[34] J. M. Sánchez-Torres, Herramientas de software especializadas para Vigilancia Tecnológica e Inteligencia Competitiva en la práctica. Guía de aplicación, 2017.

[35] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, y S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review", Information and Software Technology, vol. 51, no. 1. pp. 7-15, 2009, doi: 10.1016/j.infsof.2008.09.009

[36] K. Benyekhlef, A tale of Cyberjustice: A modern approach to technology in the Canadian Justice System. Canadá: Cyberjustice Laboratory, 2018.

[37] B. J. Mclaughlin, "Cybersecurity: Protecting Court Data Assets", en Trends in State Courts, 2018, pp. 67-72.

[38] K. Palmgren, "The use of Online Dispute Resolution: How to best integrate an online Court into the Victorian Public Justice System", 2018.

[39] A. Ganesin, L. Supayah, y I. Jamaludi, "An overview of cyber security challenges in 22 M. P. Rodríguez-Márquez developing world", Kuwait Chapter Arab. J. Bus. Manag. Rev., vol. 6, no. 4, pp. 11-20, 2016.

[40] L. Pijnenburg-Muller, "Cyber Security Capacity Building in Developing Countries", Norwegian Institute of International Affairs, NUPI Report no. 3, 2015.

[41] D. Norris Rodin y D. N. Rodin, "The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and The Federal Government", Public Contract Law J., vol. 44, no. 3, pp. 505- 528, 2015, doi: 10.2307/26419479

[42] N. Maestropiedra, "Carga de datos contextuales para el análisis y gestión del proceso judicial", en Simposio Argentino de Informática y Derecho, 2012, pp. 47–56.

[43] E. Bellone, "Videoconferencing in the Courts: An Exploratory Study of Videoconferencing Impact on the Attorney-Client Relationship in Massachusetts", tesis doctoral, Northeastern University, 2015.

[44] R. Davis *et al.*, "Research on Videoconferencing at Post-Arraignment Release Hearings: Phase I Final Report, Executive Summary", NCJRS, pp. 1-47, 2015.

[45] R. Lillo Lobos, "El Uso de Nuevas Tecnologías en el sistema Judicial: experiencias y precauciones", en Buenas prácticas para la implementación de soluciones tecnológicas en la administración de justicia, J. A. Caballero, C. G. de Grácia, and L. Hammergren, Eds. IIJusticia, 2011, pp. 117-140.

[46] Consejo Superior de la Judicatura, Acuerdo No. PSAA14-10161. Bogotá, Colombia, 2014, pp. 12.

[47] D. Devoe y S. Frattaroli, "Videoconferencing in the Courtroom: benefits, concerns, and how to move forward", 2006. [En línea]. Disponible en: http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url_r=/pu.

[48] G. A. Amoni Reverón, "El uso de la videoconferencia en cumplimiento del principio de inmediación procesal", Rev. Ius, vol. 7, no. 31, pp. 67-85, 2013, doi: 10.35487/rius.v7i31.2013.21

[49] B. Aubert, G. Babin, y H. Aqallal, "Providing an Architecture Framework for Cyberjustice", Laws, vol. 3, no. 4, pp. 721-743, 2014, doi: 10.3390/laws3040721

[50] K. Mania, "Online dispute resolution: The future of justice", Int. Comp. Jurisprud., vol. 1, no. 1, pp. 76-86, 2015, doi: 10.1016/j.icj.2015.10.006

[51] B. A. Jackson *et al.*, "Conclusions", en Fostering Innovation in the U.S. Court System., B. A. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, and N. J. Johnson, Eds. RAND Corporation, 2016, pp. 71-76.

[52] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, y M. E. Lesk, "Privacy and cybersecurity: The next 100 years", Proc. IEEE, vol. 100, pp. 1659-1673, 2012, doi: 10.1109/JPROC.2012.2189794

[53] B. Jackson *et al.*, "From Courts Today to Courts Tomorrow: Identifying and Prioritizing Innovation Needs in Technology, Policy, and Practice", en Fostering Innovation in the U.S. Court System, B. A. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, and N. J. Johnson, Eds. RAND Corporation, 2016, pp. 45-69.

[54] B. Jackson *et al.*, "The State of the U.S. Court System Today", en Fostering Innovation in the U.S. Court System, B. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, and N. J. Johnson, Eds. RAND Corporation, 2016, pp. 5-17.

[55] H. Akın Ünver, "Politics of Digital Surveillance, National Security and Privacy", Cyber Gob. Digit. Democr. pp. 1-33, 2018.

[56] N. Vermeys y M. Acevedo-Lanas, "L'émergence et l'évolution des tribunaux virtuels au Canada – L'exemple de la Plateforme d'aide au règlement des litiges en ligne (PARLe)", Rev. Jurid. la Sorbonne, vol. 1, pp. 22-51, 2020.

[57] J. S. Hollywood, J. E. Boon, R. Silberglitt, B. G. Chow, y B. A. Jackson, "Findings and Recommendations", en High-Priority Information Technology Needs for Law Enforcement, no. May 2020, RAND Corporation, 2015, pp. 51-64.

[58] L. Hammergren, “La Gobernanza Judicial y el uso de Tecnologias de la Información y la Comunicación”, en Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia, J. A. Caballero, C. G. Gracia, and L. Hammergren, Eds. IIJusticia, 2011, pp. 11-26.

[59] E. Rincón-Cárdenas, Tecnología y Administración de Justicia en Colombia. Bogotá: Colombia Digital, 2013.

[60] N. Vermeys, “Privacy v. Transparency: How Ciberse 23 guridad en la justicia digital. Recomendaciones para el caso colombiano. Remote Access to Court Records Forces Us to Re-examine Our Fundamental Values”, en eAccess to Justice, K. Benyekhlef, J. Bailey, J. Burkell, and F. Gélinas, Eds. Ottawa, Canada: University of Ottawa Press - JSTOR, 2016.

[61] M. E. Bonfanti, “Enhancing cybersecurity by safeguarding information privacy. The European Union and the implementation of the _data protection by design‘ approach”, en ACM International Conference Proceeding Series, vol. 64, pp. 1-6, 2018, doi: 10.1145/3230833.3233289

[62] J. Tomlinson, “How digital administrative justice is made”, en Justice Digit. State, 2019, pp. 63-88, doi: 10.2307/j.ctvndv808.10

[63] J. R. Clark, Federal Support and Guidance in the Establishment of Information Sharing Environments: Mid-Atlantic Regional Information Sharing (MARIS) Case Study. Washington, DC, USA: The George Washingtom University: Center for Cyber & Homeland Securoty, 2017.

[64] J. Rico-Pinto y J. M. Sánchez-Torres, “Characterization of G2G Interoperability Factors”, en ECDG 2019 19th European Conference on Digital Government, 2019, pp. 107-115.

[65] J. V. Treglia y J. S. Park, “Towards trusted intelligence information sharing”, en Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics, CSI-KDD in Conjunction with SIGKDD’09, 2009, pp. 45-52, doi: 10.1145/1599272.1599283

[66] B. Hogeveen, “Implementing e-government and digital government capabilities in the Pacific”, en ICT for development in the pacific islands, Australian Strategic Policy Institute, 2020, pp. 44-46.

[67] D. Banks, J. S. Hollywood, D. Woods, P. W. Woodson, y N. J. Johnson, “Full List of Court Needs”, en Fostering Innovation in the U.S. Court System. Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes, RAND Corporation, 2016, pp. 101-128.

[68] M. Stockman, “Insider hacking: Applying situational crime prevention to a new whitecollar crime”, en RIIT 2014 - Proceedings of the 3rd Annual Conference on Research in Information Technology, 2014, pp. 53-56, doi: 10.1145/2656434.2656436

[69] C. Zimmerman, “An Evaluation of PrivateSector Digital Forensics Processes and Practices”, tesis de maestría, City University of New York, 2013.

[70] L. Bachman, “How to take advantage of Courtroom Technology”, Iwitness, vol. 40, no. 2, pp. 14-16, 2014.

[71] J. S. Hollywood, J. E. Boon, R. Silberglitt, B. G. Chow, y B. A. Jackson, “Information Technology needs for Law Enforcement”, en High-Priority Information Technology Needs for Law Enforcement, RAND Corporation, 2015, pp. 25-49.

[72] J. S. Hollywood, D. Woods, A. Lauland, B. A. Jackson, y R. Silberglitt, “Emerging Technology Trends and Their Impact on Criminal”, RAND Corporation, pp. 1-4, 2018.

[73] M. Clifford y K. Kinloch, “The use of computer simulation evidence in court”, Comput. Law Secur. Rep., vol. 24, no. 2, pp. 169-175, 2008, doi: 10.1016/j.clsr.2007.11.002

[74] J. Horan y S. Maine, “Criminal Jury Trials in 2030: A Law Odyssey”, J. Law Soc., vol. 41, no. 4, pp. 551-575, 2014.

[75] J. S. Hollywood, D. Woods, R. Silberglitt, B. A. J. Book, y B. A. Jackson, “Using Future Internet Technologies to Strengthen Criminal Justice”, en Using Future Internet Technologies to Strengthen Criminal Justice, 2015, pp. 1-33.

[76] M. M. Lanier y A. T. Cooper, “From papyrus to cyber: how technology has directed law enforcement policy and practice”, Crim. Justice Stud., vol. 29, no. 2, pp. 92-104, 2016, doi: 10.1080/1478601X.2016.1170280

[77] E. Kalemi y S. Yildirim-yayilgan, “Ontologies for Social Media Digital Evidence”, Int. J. Comput. Electr. Autom. Control Inf. Eng., vol. 10, no. 2, pp. 324-329, 2016.

[78] U. Ewald, "Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches?", en Proceedings of the Third Central European Cybersecurity Conference, 2019, pp. 281--282, doi: 10.1145/3360664.3362697

[79] F. Coudert, D. Butin, y D. Le Métayer, "Body-worn cameras for police accountability: Opportunities and risks", Comput. Law Secur. Rev., vol. 31, no. 6, pp. 749-762, 2015, doi: 10.1016/j.clsr.2015.09.002

[80] M. Cukier, D. Maimon, y R. Berthier, "A journey towards rigorous cybersecurity experiments: On the application of criminological theories", en ACM International Conference Proceeding Series - Learning from Authoritative Security Experiment Results, LASER 2012, pp. 25-30, doi: 10.1145/2379616.2379620

[81] S. E. Goodison, R. C. Davis, y B. Jackson, "Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize 24 M. P. Rodríguez-Márquez Digital Evidence", en Digital Evidence and the U.S. Criminal Justice System, RAND Corporation, 2015, pp. 1-32.

[82] B. A. Jackson *et al.*, "Court Technology and Practice Today", en Fostering Innovation in the U.S. Court System. Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes, B. A. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, and N. J. Johnson, Eds. RAND Corporation, 2016, pp. 19-43.

[83] N. Aletras, D. Tsarapatsanis, D. Preoţiuc-Pietro, y V. Lampos, "Predicting judicial decisions of the European court of human rights: A natural language processing perspective", PeerJ Comput. Sci., vol. 2016, no. 10, pp. 1-19, 2016, doi: 10.7717/peerj-cs.93

[84] E. Estevez, P. Fillotrani, y S. Linares Lejarraga, PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial. Washington, DC, USA: Banco Interamericano de Desarrollo, 2020, doi: 10.18235/0002378

[85] C. Li, Y. Sheng, J. Ge, y B. Luo, "Apply event extraction techniques to the judicial field", en UbiComp/ISWC 2019- Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers, 2019, pp. 492-497, doi: 10.1145/3341162.3345608

[86] C. Prins, "Digital justice", Comput. Law Secur. Rev., vol. 34, no. 4, pp. 920-923, 2018, doi: 10.1016/j.clsr.2018.05.024

[87] D. Martin Katz, M. J. Bommarito, y J. Blackman, "A general approach for predicting the behavior of the Supreme Court of the United States", PLoS One, vol. 12, no. 4, pp. 1-18, 2017, doi: 10.1371/journal.pone.0174698

[88] H. Westermann, V. R. Walker, K. D. Ashley, y K. Benyekhlef, "Using factors to predict and analyze landlord-tenant decisions to increase access to Justice", en Proc. 17th Int. Conf. Artif. Intell. Law, ICAIL 2019, pp. 133-142, doi: 10.1145/3322640.3326732

[89] O. M. Şulea, M. Zampieri, M. Vela, y J. Van Genabith, "Predicting the law area and decisions of French supreme court cases", Int. Conf. Recent Adv. Nat. Lang. Process. RANLP, vol. 2017-Sep, pp. 716-722, 2017, doi: 10.26615/978-954-452-049-6-092

[90] & S. K. NU., GK., GS., RamasubramanianK., "The LAWBO: A Smart Lawyer Chatbot: AI Assisted System to scan past judgement to recommend appropriate IPC rules for case preparation", Probyto J. AI Res., vol. 1, no. 1, 2020.

[91] S. Castell, "The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision?", Comput. Law Secur. Rev., vol. 34, no. 4, pp. 739-753, 2018, doi: 10.1016/j.clsr.2018.05.011

[92] E. Rincón-Cárdenas, "Justicia y TICs, desde el Plan Nacional de TIC, Articulación de una Política Pública", en Tecnologías al servicio de la Justicia y el Derecho, Bogotá, Colombia: Pontificia Universidad Javeriana, 2019, pp. 71-102.

[93] M. Da Luz Batalha, "Government and army policies toward cybernetic security and defense in Brazil", en ACM International Conference Proceeding Series, 2013, pp. 265-266, doi: 10.1145/2479724.2479765

[94] R. Mcmillion, "It's Not Just the Economy: The 113th Congress will face a full agenda of issues relating to the justice system", ABA J., vol. 99, pp. 62, 2013.

[95] S. M. T. Toapanta, A. J. Gurumendi, y L. E. M. Gallegos, "An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of Ecuador", en ACM International Conference Proceeding Series ICETEM 2019, pp. 61-66, doi: 10.1145/3375900.3375909

[96] F. D. Kramer y R. J. Butler, "A roadmap to better cybersecurity", en Cybersecurity: Changing the model, Atlantic Council, 2019, pp. 5-20.

[97] M. E. Sánchez-Acevedo, "Estrategia jurídica para la gestión, análisis y ciberseguridad de la información en la investigación penal", tesis de maestría, Escuela Superior de Guerra General Rafael Reyes Prieto, 2017.

[98] R. Duaso-Calés, "Justicia electrónica y privacidad: nuevas pistas de reflexión sobre la cuestión de la protección de los datos personales y la publicación de las sentencias judiciales en Internet", en Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia, 2011, pp. 177-191.

[99] A. T. Chatfield y C. G. Reddick, "Cybersecurity innovation in government: A case study of U.S. Pentagon's vulnerability reward program", en ACM International Conference Proceeding Series, 2017, pp. 64-73, doi: 10.1145/3085228.3085233

[100] Grupo e-justicia - Cumbre Judicial Iberoaméricana, "Recomendaciones sobre Ciberseguridad", en XIX Edición – Cumbre Judicial Iberoamericana Abril, Quito, 2018.

[101] Center for Cyber and Homeland Security., Cybersecurity for State and Local Law Enforcement: A Policy Roadmap to Enhance Capabilities. Washington, DC, USA: Centro de seguridad cibernética y nacional, Universidad George Washington, 2016.

[102] N. W. Vermeys y K. Benyekhlef, "Best Practices in the Field of Cyberjustice", en Buenas prácticas para la implementación de soluciones tecnológicas en la Administración de Justicia, México, DF: IIJusticia, 2011.

[103] J. Bailey, "INTRODUCTION- Fundamental Values in a Technologized Age of Efficiencyannotated", en eAcces to Justice, K. Benyekhlef, J. Bailey, J. Burkell, and F. Gélinas, Eds. University of Ottawa Press - JSTOR, 2016, pp. 25-27.

[104] A. Aspis, "Las TICs y el Rol de la Justicia en Latinoamérica", Derecho Soc., vol. 0, no. 35, pp. 327-340, 2010.

[105] P. Fabra-i-Abat, A. Battle-Rubio, A. CerrilloMartínez, A. Galiano-Barajas, I. Peña-Lopez, y C. Colombo-Vilarrasa, eJusticia: la justicia en la sociedad del conocimiento. retos para los países iberoamericanos. Santo Domingo, 2006.

[106] K. Morales-Navarro, "La inclusión de las tecnologías en la gestión judicial Poder Judicial de República de Costa Rica", en El rol de las Nuevas Tecnologías en el Sistema de Justicia, C. Riego and A. Binder, Eds. Publicación semestral del Centro de Estudios de Justicia de las Américas – CEJA, Año 9, Nº 162011, pp. 48-55.

[107] T. Rojas Quispe, "La notificación virtual y su implementación en la Administración de Justicia en el Perú", Rev. Científica Jurídica SSIAS. Investig. Jurídica, vol. 7, no. 1, pp. 1-19, 2014.

[108] C. Quispe Angulo, "El expediente digital y su incidencia en la administración de justicia en el Perú", tesis de grado, Universidad Señor de Sipán, 2018.

[109] A. Freire Pimentel, C. P. Mateus, y P. Mendes Saldanha, "El proceso judicial electrónico, la seguridad jurídica y violaciones de los derechos fundamentales desde el punto de vista del sistema jurídico brasileño", Rev. Derecho, Comun. y Nuevas Tecnol., no. 17, pp. 1-19, 2017.

[110] R. J. Á. Chávez, "El Modelo del Sistema de Justicia en Línea y su expansión a otros ámbitos de la jurisdicción", en El derecho mexicano contemporáneo: Retos y dilemas, D. C. Salgado y J. B. Quinto, Universidad Nacional Autónoma de México: Instituto de Investigaciones Jurídicas pp. 197-212, 2011.

[111] Asamblea Legislativa El Salvador, Decreto 146 de 2015. El Salvador, 2015.

[112] A. de los A. Ríos Ruiz, "La Justicia electrónica en México: Visión comparada con América Latina", Revista de la facultad de derecho de México, vol. 67, no. 266, pp. 389-422, 2017, doi: 10.22201/fder.24488933e.2016.266.59011

[113] J. Caballero, G. de Gracia, y L. Hammergren, Buenas Prácticas para la implementación de soluciones tecnológicas en la Administración de Justicia. Mexico, DF: IIJusticia, 2011.

[114] R. Beauchard, "Cyberjustice and International Development: Reducing the gap between Promises and Accomplishments", en eAccess to Justice, K. Benyekhlef, J. Bailey, and J. Burkell, Eds. Ottawa, Canada: University of Ottawa Press - JSTOR, 2016.

[115] R. Susskind, Online Courts and the Future of Justice. Oxford, Inglaterra: Oxford University Press, 2019.

[116] GRUPO E-JUSTICIA, "Recomendaciones sobre Ciberseguridad", en Cumbre Judicial Iberoamericana Edición XIX, 2018.

[117] Consejo Superior de la Judicatura, Plan de desarrollo de la Justicia 1995-1998. Bogotá, Colombia, 1994.

[118] G. S. López-Jaramillo, "Nuevo modelo de justicia en línea colombiano", en Tecnologías al servicio de la Justicia y el Derecho, Bogotá, Colombia: Pontificia Universidad Javeriana, 2019, pp. 37-58.

[119] E. Gil Botero, "Las TIC como logro para una justicia moderna", en Tecnologías al servicio de la Justicia y el Derecho, Bogotá, Colombia: Pontificia Universidad Javeriana, 2019, pp. 59-69.

[120] Presidencia de la República de Colombia, Decreto 806 de 2020. Bogotá, 2020, pp. 21.

[121] M. Hilbert, "Toward a Conceptual Framework for ICT for Development: Lessons Learned from the Latin American _Cube Framework", Inf. Technol. Int. Dev., vol. 8, no. 4, pp. 243-259, 2012.

[122] INPEC - Subdirección de Planeación, "Reporte de Audiencias virtuales", documento interno de trabajo, Bogotá, 2019.